PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091828
(43)Date of publication of application : 29.03.2002

(51)Int.Cl. G06F 12/14
G06F 1/00
G09C 1/00
G11B 20/10

(21)Application number : 2000-282720
(22)Date of filing : 18.09.2000

(71)Applicant : SHARP CORP
(72)Inventor : KAWA NORIAKI

(54) DATA PROCESSORSTORAGE DEVICE AND DATA TRANSFER SYSTEM USING THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To surely prevent data stored in a storage device from being illegally copied.
SOLUTION: A data processor 2 is provided with a processing part 21 for outputting an address for designating data to be processed by the data processor 2 in data stored in a storage device 1 and an encoder/decoder 22 for encoding the address outputted from the processing part 31sending the encoded address to the storage device 1receiving encoded data from the storage device 1 and decoding the encoded data. The encoder/decoder 22 is provided with setting parts (36 and 24) for receiving ID information peculiar to the storage device 1 from the storage device 1 and setting an initial value and logical operation on the basis of the ID informationencoding/decoding KEY generating parts (25 and 27) for generating an encoding/decoding KEY by performing the set logical operation to the set initial valuean encoding part 29 for encoding the address on the basis of the encoding/decoding KEY and a decoding part 28 for decoding the encoded data on the basis of the encoding/decoding KEY.

CLAIMS

[Claim(s)]
[Claim 1]A treating part which outputs an address which specifies data which should be processed by said data processing device among data which is

removable data processing devices and was memorized by said memory storage in memory storageEncipher said address outputted from said treating partand said enciphered address is sent to said memory storageReceive data enciphered from said memory storagehave encryption/decryption machine which decrypts said enciphered dataand said encryption/decryption machineBy receiving ID information peculiar to said memory storage from said memory storageand performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID informationand said set-up initial valueA data processing device containing an encryption/decryption KEY generation part which generates encryption / decryption KEYan encryption section which enciphers said address based on said encryption / decryption KEYand a decoding section which decrypts said enciphered data based on said encryption / decryption KEY.

[Claim 2]The data processing device according to claim 1 received in the state where said set part is not having said ID information enciphered when said data processing device is equipped with said memory storage.

[Claim 3]The data processing device according to claim 1 with which said encryption/decryption KEY generation part updates said encryption / decryption KEY periodically or irregularly.

[Claim 4]By performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said addresssaid encryption section enciphers and said address said decoding sectionThe data processing device according to claim 1 which decrypts said enciphered data by performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said enciphered data.

[Claim 5]The data processing device comprising according to claim 1:

A shift register to which said encryption/decryption KEY generation part holds data containing two or more bitsand said data is shifted according to a shift clock.

A feedback equivalent logic formation part which performs an alternative exclusive OR (EOR) operation according to said set-up logical operation to said data currently held at said shift registerand feeds back the result of an operation to an input of said shift register.

[Claim 6]The data processing device according to claim 5 which generates said encryption / decryption KEY when said encryption/decryption KEY generation part rearranges bit order of said data currently held at said shift register in the given order.

[Claim 7]The data processing device according to claim 5 which generates new encryption / decryption KEY when said encryption/decryption KEY generation part changes the number of times which shifts said data currently held at said shift register.

[Claim 8]Memory storage which can be desorbed to a data processing device characterized by comprising the following.

A storage parts store which is a storage parts store data was remembered to beand outputs data corresponding to an address.

Receive an address enciphered from said data processing deviceand said enciphered address is decryptedEncipher said data outputted from said memory storagehave encryption/decryption machine which sends said enciphered data to said data processing deviceand said encryption/decryption machineAn encryption/decryption KEY generation part which generates encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storage.
A decoding section which decrypts said enciphered address based on said encryption / decryption KEY.
An encryption section which enciphers said data outputted from said memory storage based on said encryption / decryption KEY.

[Claim 9]The memory storage according to claim 8 with which said encryption/decryption KEY generation part updates said encryption / decryption KEY periodically or irregularly.
[Claim 10]Said decoding section by performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said enciphered addressThe memory storage according to claim 8 which enciphers said data when said enciphered address is decrypted and said encryption section performs an exclusive OR (EOR) operation to said encryption / decryption KEYand said data.
[Claim 11]The memory storage comprising according to claim 8:
A shift register to which said encryption/decryption KEY generation part holds data containing two or more bitsand said data is shifted according to a shift clock.
A feedback part which performs an alternative exclusive OR (EOR) operation beforehand set up based on said ID information to said data currently held at said shift registerand feeds back the result of an operation to an input of said shift register.

[Claim 12]The memory storage according to claim 11 with which said data currently held at said shift register is initialized by initial value beforehand set up based on said ID information.
[Claim 13]The memory storage according to claim 11 which generates said encryption / decryption KEY when said encryption/decryption KEY generation part rearranges bit order of said data currently held at said shift register in the given order.
[Claim 14]The memory storage according to claim 11 which generates new encryption / decryption KEY when said encryption/decryption KEY generation part changes the number of times which shifts said data currently held at said shift register.
[Claim 15]The memory storage according to claim 8 currently formed on a semiconductor chip with single said storage parts store and said encryption/decryption machine.
[Claim 16]Are a data processing device and memory storage removable to said data processing device the data transfer system which it hadand said data

processing deviceA treating part which outputs an address which specifies data which should be processed by said data processing device among data memorized by said memory storageEncipher said address outputted from said treating partand said enciphered address is sent to said memory storageReceive data enciphered from said memory storagehave 1st encryption/decryption machine that decrypts said enciphered dataand said 1st encryption/decryption machineBy receiving ID information peculiar to said memory storage from said memory storageand performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID informationand said set-up initial valueThe 1st encryption/decryption KEY generation part that generates the 1st encryption / decryption KEYIt is the storage parts storeas for said memory storagedata was remembered to be including the 1st encryption section that enciphers said address based on said the 1st encryption / decryption KEYand the 1st decoding section that decrypts said enciphered data based on said the 1st encryption / decryption KEYA storage parts store which outputs data corresponding to said addressand an address enciphered from said data processing device are receivedDecrypt said enciphered address and said data outputted from said memory storage is encipheredHave 2nd encryption/decryption machine that sends said enciphered data to said data processing deviceand said 2nd encryption/decryption machineThe 2nd encryption/decryption KEY generation part that generates the 2nd encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storageA data transfer system containing the 2nd decoding section that decrypts said enciphered address based on said the 2nd encryption / decryption KEYand the 2nd encryption section that enciphers said data outputted from said memory storage based on said the 2nd encryption / decryption KEY.

[Claim 17]The data transfer system according to claim 16 generated according to logic with equivalent said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY.

[Claim 18]The data transfer system according to claim 16 with which said data processing device is further provided with a control section which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine at least.

[Claim 19]When said data processing device is equipped with said memory storagesaid control sectionSo that said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY may be reset and said the 1st same encryption / decryption KEYand said the 2nd encryption/decryption KEY may be generated based on said ID informationThe data transfer system according to claim 18 which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the data processing device and memory storage which prevent the program memorized by memory storage removable to a data processing deviceand data from being reproduced unjustlyand a data transmission system.
[0002]
[Description of the Prior Art]The dismountable semiconductor memory device (for exampleROM) is supplied to the commercial scene in large quantities in the form of a home video game cassette etc. from the data processing device today. Supposing it does not take the measure against unjust copy protectionthere is a possibility that the pirate edition of a game cassette may appear on the market in a commercial scene in large quantities.
[0003]How to prevent the data memorized by the semiconductor memory device from being reproduced unjustly conventionallyOr using the data reproduced unjustly as a method of making it impossible or difficult(1) Before reading the method of memorizing the enciphered data to a semiconductor memory deviceand the data memorized by (2) semiconductor memory devicesthe method of performing performs authentication which checks that a semiconductor memory device or a data processing device is regular is known.
[0004]For exampleJPS60-167033AJPS61-67136Aand JPH5-53921A are indicating the method of memorizing the enciphered data to a semiconductor memory device.
[0005]For exampleafter performing performs authentication which checks that JPH6-168185A and the patent No. 2698371 gazette have a regular data processing device with which it is equipped with a semiconductor memory devicethe method of reading the data memorized by the semiconductor memory device is indicated.
[0006]
[Problem(s) to be Solved by the Invention]In the method of memorizing the enciphered data to a semiconductor memory devicesince the data itself memorized by the semiconductor memory device is encipheredthe change use of data and the surreptitious use of a program which were read from the semiconductor memory device can be prevented. Howeverin this methodthe enciphered data which is memorized by the semiconductor memory device cannot be prevented from being reproduced unjustly.
[0007]In the method of performing performs authentication which checks a data processing device being regularthe data memorized by the semiconductor memory device using the data processing device which is not regular can be prevented from being reproduced unjustly. Howeverin this methodsince it is possibleobserving and (probe) reading the data which is transmitted between a semiconductor memory device and a data processing device and which is not enciphered cannot prevent certainly surreptitious use of the data memorized by the semiconductor memory device and a program.
[0008]How to encipher communications on the opened networksuch as wireless

information communicationis also known. For exampleJPH6-342257A and JPH8-307411AEncryption / decryption KEY (key) is generated based on the pseudo-random number which made it generate combining LFSR (linear feedback shift register)and the method of enciphering commo data based on this encryption / decryption KEY (key) is indicated. Encoding technology given in these gazettes is the art about secret communication. Using such encoding technology for the purpose of preventing the data memorized by the semiconductor memory device from being reproduced unjustly is not suggested to these gazettes.
[0009]This invention is made in order to solve the problem mentioned aboveand it is a thing.
the purpose is to provide the data processing device and memory storage which prevent the program which is alike and is memorized by removable memory storageand data from being reproduced unjustlyand a data transmission system.

[0010]
[Means for Solving the Problem]A treating part which outputs an address which specifies data in which a data processing device of this invention should be processed by said data processing device in memory storage among data which is removable data processing devices and was memorized by said memory storageEncipher said address outputted from said treating partand said enciphered address is sent to said memory storageReceive data enciphered from said memory storagehave encryption/decryption machine which decrypts said enciphered dataand said encryption/decryption machineBy receiving ID information peculiar to said memory storage from said memory storageand performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID informationand said set-up initial valueAn encryption/decryption KEY generation part which generates encryption / decryption KEYand an encryption section which enciphers said address based on said encryption / decryption KEYTherebythe above-mentioned purpose is attained including a decoding section which decrypts said enciphered data based on said encryption / decryption KEY.
[0011]Said set part may be received in the state where said ID information is encipheredwhen said data processing device is equipped with said memory storage.
[0012]Said encryption/decryption KEY generation part may update said encryption / decryption KEY periodically or irregularly.
[0013]By performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said addresssaid encryption section enciphers and said address said decoding sectionSaid enciphered data may be decrypted by performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said enciphered data.
[0014]A shift register to which said encryption/decryption KEY generation part holds data containing two or more bitsand said data is shifted according to a shift clockAn alternative exclusive OR (EOR) operation according to said set-up logical operation may be performed to said data currently held at said shift registerand a feedback equivalent logic formation part which feeds back the result of an

operation to an input of said shift register may be included.
[0015]Said encryption/decryption KEY generation part may generate said encryption / decryption KEY by rearranging bit order of said data currently held at said shift register in the given order.
[0016]Said encryption/decryption KEY generation part may generate new encryption / decryption KEY by changing the number of times which shifts said data currently held at said shift register.
[0017]A storage parts store which memory storage of this invention is the memory storage which can be desorbed to a data processing deviceis a storage parts store data was remembered to beand outputs data corresponding to an addressReceive an address enciphered from said data processing deviceand said enciphered address is decryptedEncipher said data outputted from said memory storagehave encryption/decryption machine which sends said enciphered data to said data processing deviceand said encryption/decryption machineAn encryption/decryption KEY generation part which generates encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storageTherebythe above-mentioned purpose is attained including a decoding section which decrypts said enciphered address based on said encryption / decryption KEYand an encryption section which enciphers said data outputted from said memory storage based on said encryption / decryption KEY.
[0018]Said encryption/decryption KEY generation part may update said encryption / decryption KEY periodically or irregularly.
[0019]Said decoding section by performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said enciphered addressSaid encryption section may encipher said data by decrypting said enciphered address by performing an exclusive OR (EOR) operation to said encryption / decryption KEYand said data.
[0020]A shift register to which said encryption/decryption KEY generation part holds data containing two or more bitsand said data is shifted according to a shift clockAn alternative exclusive OR (EOR) operation beforehand set up based on said ID information to said data currently held at said shift register may be performedand a feedback part which feeds back the result of an operation to an input of said shift register may be included.
[0021]Said data currently held at said shift register may be initialized by initial value beforehand set up based on said ID information.
[0022]Said encryption/decryption KEY generation part may generate said encryption / decryption KEY by rearranging bit order of said data currently held at said shift register in the given order.
[0023]Said encryption/decryption KEY generation part may generate new encryption / decryption KEY by changing the number of times which shifts said data currently held at said shift register.
[0024]It may be formed on a semiconductor chip with single said storage parts store and said encryption/decryption machine.

[0025]A data transfer system of this invention is a data processing device and memory storage removable to said data processing device a data transfer system which it hadand said data processing deviceA treating part which outputs an address which specifies data which should be processed by said data processing device among data memorized by said memory storageEncipher said address outputted from said treating partand said enciphered address is sent to said memory storageReceive data enciphered from said memory storagehave 1st encryption/decryption machine that decrypts said enciphered dataand said 1st encryption/decryption machineBy receiving ID information peculiar to said memory storage from said memory storageand performing said set-up logical operation to a set part which sets up an initial value and a logical operation based on said ID informationand said set-up initial valueThe 1st encryption/decryption KEY generation part that generates the 1st encryption / decryption KEYIt is the storage parts storeas for said memory storagedata was remembered to be including the 1st encryption section that enciphers said address based on said the 1st encryption / decryption KEYand the 1st decoding section that decrypts said enciphered data based on said the 1st encryption / decryption KEYA storage parts store which outputs data corresponding to said addressand an address enciphered from said data processing device are receivedDecrypt said enciphered address and said data outputted from said memory storage is encipheredHave 2nd encryption/decryption machine that sends said enciphered data to said data processing deviceand said 2nd encryption/decryption machineThe 2nd encryption/decryption KEY generation part that generates the 2nd encryption / decryption KEY based on ID information peculiar to said memory storage beforehand set as said memory storageTherebythe above-mentioned purpose is attained including the 2nd decoding section that decrypts said enciphered address based on said the 2nd encryption / decryption KEYand the 2nd encryption section that enciphers said data outputted from said memory storage based on said the 2nd encryption / decryption KEY.

[0026]It may be generated according to logic with equivalent said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY.

[0027]Said data processing device may be further provided with a control section which controls said 1st encryption/decryption machine and said 2nd encryption/decryption machine at least.

[0028]When said data processing device is equipped with said memory storagesaid control sectionSo that said the 1st encryption / decryption KEYand said the 2nd encryption/decryption KEY may be reset and said the 1st same encryption / decryption KEYand said the 2nd encryption/decryption KEY may be generated based on said ID informationSaid 1st encryption/decryption machine and said 2nd encryption/decryption machine may be controlled.

[0029]

[Embodiment of the Invention]Hereafteran embodiment of the invention is describedreferring to Drawings.

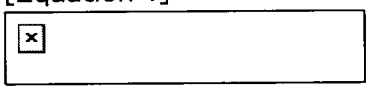
[0030]Drawing 1 shows the example of composition of the data transfer system

100 of an embodiment of the invention.
[0031]The data transfer system 100 is provided with the following.
Memory storage 1.
Data processing device 2.
The memory storage 1 is constituted by the data processing device 2 removable. The data processing device 2 is equipped with the one memory storage 1 chosen from two or more memory storage of the same standard.
[0032]The data processing device 2 outputs the address enciphered by the memory storage 1 with which it was equipped. The memory storage 1 outputs the enciphered data corresponding to the enciphered address to the data processing device 2. Thusit becomes difficult to get to know the contents of the data memorized by the memory storage 1 from data transmitting by enciphering the address and data which are transmitted between the memory storage 1 and the data processing device 2.
[0033]The memory storage 1 is the game cassette for home video games in which a game program and various data were memorizedfor example. The data processing device 2 is a home video game machinefor example. The home video game machine has an opening for equipping with a game cassette. If the opening of a home video game machine is equipped with a game cassettethe game program and various data which are memorized by the game cassette will be read to a home video game machineand a game screen will be displayed on the display of the television etc. which are connected to the home video game machine.
[0034]The memory storage 1 is provided with the following.
Storage parts store 10.
Encryption/decryption machine 11.
As for the storage parts store 10 and encryption/decryption machine 11it is preferred to be formed on a single semiconductor chip (for examplesilicon chip).
[0035]ID information (for exampleID number) peculiar to the memory storage 1and a program and various data are beforehand memorized by the storage parts store 10. ID information is a lot number assigned to every [of the same standard] memory storage (product)for example. Or ID information may be the value chosen from two or more values. ID information is memorized to the predetermined address (for example0th street) of the storage parts store 10. The storage parts store 10 receives an address from encryption/decryption machine 11and outputs the data memorized by the position corresponding to the address to encryption/decryption machine 11.
[0036]In this Descriptionthe term "data" is understood as a comprehensive term which shall mean the information arbitrary type which may be memorized by the storage parts store 10and contains a program and various data.
[0037]Encryption/decryption machine 11 receives the enciphered address from the data processing device 2and generates an address by decrypting the enciphered address. The address is outputted to the storage parts store 10. Encryption/decryption machine 11 receives the data outputted from the storage parts store 10and generates the data enciphered by enciphering the data. The

enciphered data is outputted to the data processing device 2.
[0038]The data processing device 2 is provided with the following.
Treating part 21.
Encryption/decryption machine 22.

[0039]If the data processing device 2 is equipped with the memory storage 1encryption/decryption machine 11 in the memory storage 1 and encryption/decryption machine 22 in the data processing device 2 will be in the state where it was electrically connected mutually. For exampleencryption/decryption machine 11 and encryption/decryption machine 22 of each other may electrically be connected via a connector (not shown).
[0040]The treating part 21 outputs the address which specifies the data which should be processed by the data processing device 2 among the data memorized by the memory storage 1.
[0041]Encryption/decryption machine 22 receives the address outputted from the treating part 21and generates the address enciphered by enciphering the address. The enciphered address is outputted to the memory storage 1.
Encryption/decryption machine 22 receives the enciphered data which was outputted from the memory storage 1and generates data by decrypting the enciphered data. The data is outputted to the treating part 21.
[0042]The data processing device 2 contains further the control section 20 which controls encryption/decryption machine 11encryption/decryption machine 22and the treating part 21.
[0043]The control section 20 contains the code generation controller 23. The code generation controller 23 so that the timing of generation of the encryption / decryption KEY in encryption/decryption machine 11the timing of change and generation of the encryption / decryption KEY in encryption/decryption machine 22and change may synchronizeEncryption/decryption machine 11 and encryption/decryption machine 22 are controlled.
[0044]The code generation controller 23 supplies a control signal common to encryption/decryption machine 11 and encryption/decryption machine 22 to encryption/decryption machine 11 and encryption/decryption machine 22 via the controlling signal line 41The control signal only relevant to encryption/decryption machine 22 is supplied to encryption/decryption machine 22 via the controlling signal line 42.
[0045]Drawing 2 shows the example of composition of encryption/decryption machine 11 of the memory storage 1.
[0046]Encryption/decryption machine 11 contains LFSR(Linear Feedback Shift Register)12 which generates a pseudo-random number.
[0047]LFSR12 is a circuit which performs an exclusive OR (below Exclusive OR; calls it "EOR") operation to the bit of shoes to be chosen among the data of N bit currently held at the shift registerand feeds back the result of an operation to the input of a shift register. A shift register is constituted by connecting a D flip-flop (DFF) in seriesfor example.

[0048]a maximum of [from which the characteristic differs by whether the result of an operation is fed back to which bit position of a shift register by performing an EOR operation to which bit among the data of N bit currently held at the shift register] -- the pseudorandom-numbers (pattern) sequence of the cycle of 2^N-1 can be acquired. Heregenerally the pseudo-random number sequence which has a cycle of 2^N-1 which is the maximum is called "an M sequence (Maximam length Sequences)." HereN is two or more arbitrary integers.
[0049]The Nth polynomial shown in (several 1) can express whether an EOR operation is performed to which bit among the data of N bit currently held at the shift register.
[0050]
[Equation 1]



Howeverit is referred to as $a_k=0$ when not using the k-th bit for an EOR operation among data of N bit currently held at $a_k=1$ and a shift register when using the k-th bit for an EOR operation among data of N bit currently held at a shift registerIt is referred to as $a_0=1$ and $a_N=1$. This polynomial f(x) is called a LFSR characteristic polynomialand expresses the characteristic of pseudorandom numbers which LFSR generates.
[0051]For examplewhen performing an EOR operation to the 1st bit and the 4th bit in the case of N= 4LFSR characteristic polynomial f(x) is expressed as "x^4+x+1."
[0052]Although a LFSR characteristic polynomial for forming an M sequence is restrictedin this inventionpseudo-random number sequence in particular acquired does not need to be an M sequence. Howeveras an initial value of data of N bit held at a shift registerSetting up a value (for example0...0 (ALL0)) which causes a dead loop (or stack State) from which change does not take place to data of N bit held at a shift register even if it repeats this processing must avoid.
[0053]Based on ID information memorized by the storage parts store 10an initial value and a LFSR characteristic polynomial of data of N bit which should be held at a shift register of LFSR are determined beforehand. LFSR12 is formed as a circuit which fills an initial value and a LFSR characteristic polynomial of data of the N bit determined beforehand.
[0054]Drawing 3 shows an example of composition of LFSR12. LFSR12 has the shift register 18a holding data of N bit. The shift register 18a comprises N D flip-flops (DFF) 18 connected in series.
[0055]If an initial value load signal is inputted into LFSR12data of N bit currently held at the shift register 18a will be initialized. An initial value of data of the N bit is beforehand memorized by the N registers 19. An initial value of data of the N bit is beforehand determined based on ID information memorized by the storage parts store 10. Or an initial value of data of the N bit is beforehand determined by an initial value load signal inputted into each bit of N DFF18 being connected to either an asynchronous set which is each bitor asynchronous reset.

[0056]If a shift clock is inputted into LFSR121 bit of data of N bit currently held at the shift register 18a will be shifted in the direction of every predetermined one by one. The number of times of a shift can be set as the arbitrary number of times.
[0057]A bit of some of the data of N bit currently held at the shift register 18a in accordance with a selection rule beforehand determined based on ID information memorized by the storage parts store 10 is chosenand an EOR operation is performed to a selected bit. A result of the EOR operation is fed back to an input of the 1st bit (namelythe 1st step of DFF18) of the shift register 18a. In an example shown in drawing 3an EOR operation is performed to the 1st bit and the 3rd bit among data of N bit currently held at the shift register 18aand a result of the EOR operation is fed back to an input which is the 1st bit of the shift register 18a. The EOR arithmetic element 13 is used in order to perform an EOR operation to the 1st bit and the 3rd bit.
[0058]A selection rule which specifies whether which bit of an initial value of data of N bit held at the shift register 18a and the data of N bit held at the shift register 18a is chosenand an EOR operation is performed is uniquely determined based on ID information memorized by the storage parts store 10.
[0059]Synchronizing with a shift clock with which LFSR12 is supplied from the code generation controller 23only the number of operation times M set up at random repeats shift operation and an EOR operation of the shift register 18a. Data of N bit outputted from N DFF18 contained in the shift register 18a is outputted from LFSR12 as the output data OUT after an end of repetition processing. The output data OUT expresses a pseudo-random number.
[0060]Again with reference to drawing 2the register (Key_Reg) 14 is connected to LFSR12 so that bit order of the output data OUT outputted from LFSR12 may be rearranged into predetermined bit order. Data of N bit held Key_Reg14 is considered as encryption / decryption KEY.
[0061]Bit width of the output data OUT and bit width of Key_Reg14 which are outputted from LFSR12 are the same as the larger one among bit width of data outputted from bit width and the storage parts store 10 of an address which are inputted into the storage parts store 10or it has become more than it. Thereforedata of a bit chosen among data of N bit held Key_Reg14 according to bit width of an address or bit width of data may be considered as encryption / decryption KEY.
[0062]A KEY reset signal and a KEY set clock are supplied to Key_Reg14 from the code generation controller 23. Synchronizing with a KEY reset signalthe encryption / decryption KEY currently held Key_Reg14 are reset. Synchronizing with a KEY set clockthe output data OUT outputted from LFSR12 is incorporated into Key_Reg14and is held.
[0063]A KEY set clock is outputted periodically or irregularly from the code generation controller 23. Encryption / decryption KEY answers a KEY set clockand is updated periodically or irregularly.
[0064]ThusLFSR12 and Key_Reg14 function based on ID information peculiar to the memory storage 1 beforehand set as the memory storage 1 as an

encryption/decryption KEY generation part which generates encryption / decryption KEY.
[0065]The encryption / decryption KEY held Key_Reg14 are given to the decryption EOR gate sequence 15 and the encryption EOR gate sequence 17.
[0066]The decryption EOR gate sequence 15 receives an enciphered address from the data processing device 2An enciphered address is decrypted by receiving encryption / decryption KEY from Key_Reg14and performing an EOR operation to each bit of an address and each bit of encryption / decryption KEY which were enciphered.
[0067]Thusthe decryption EOR gate sequence 15 functions as a decoding section which decrypts an address enciphered based on encryption / decryption KEY.
[0068]The EOR result of an operation by the decryption EOR gate sequence 15 is given to the selector 16. The selector 16 refers to the encryption / decryption KEY currently held Key_Reg14When encryption / decryption KEY is "ALL0" (state where all bit is "0" and encryption / decryption KEY is not set up)The 0th addressis outputted to the storage parts store 10and when encryption / decryption KEY is not "ALL0"an address outputted from the decryption EOR gate sequence 15 is outputted to the storage parts store 10.
[0069]The storage parts store 10 outputs data stored in a position corresponding to an address outputted from the selector 16.
[0070]The encryption EOR gate sequence 17 receives data outputted from the storage parts store 10Data outputted from the storage parts store 10 is enciphered by receiving encryption / decryption KEY from Key_Reg14and performing an EOR operation to each bit of data and each bit of encryption / decryption KEY which were outputted from the storage parts store 10.
[0071]Thusthe encryption EOR gate sequence 17 functions as an encryption section which enciphers data outputted from the storage parts store 10 based on encryption / decryption KEY.
[0072]As mentioned abovewhen the encryption / decryption KEY currently held Key_Reg14 are "ALL0"the selector 16 outputs "the 0th address" to the storage parts store 10 irrespective of an address outputted from the decryption EOR gate sequence 15. The storage parts store 10 outputs ID information memorized by "the 0th street" to "the 0th address." In this casethe encryption EOR gate sequence 17 will perform an EOR operation to "ALL0" and ID information. As a resultID information is outputted from the encryption EOR gate sequence 17.
[0073]Drawing 4 shows an example of composition of encryption/decryption machine 22 of the data processing device 2.
[0074]The register (ID_Reg) 36 holding ID information to which encryption/decryption machine 22 was outputted from the memory storage 1Based on ID information held ID_Reg36the LFSR initial value characteristic polynomial set part 24 which determines an initial value and a LFSR characteristic polynomial for generating a pseudo-random number is included.
[0075]If the data processing device 2 is equipped with the memory storage 1ID information will be transmitted to the data processing device 2 from the memory

storage 1. This ID information is transmitted in the state where it is not enciphered.
[0076]ID_Reg36 incorporates and holds ID information transmitted from the memory storage 1 synchronizing with ID set signal supplied from the code generation controller 23. ID information held ID_Reg36 is outputted to the LFSR initial value characteristic polynomial set part 24.
[0077]Logic used when determining an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information in the LFSR initial value characteristic polynomial set part 24In LFSR12 provided in encryption/decryption machine 11 of the memory storage 1it is equivalent to logic used when determining beforehand an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information. As opposed to a circuit which realizes an initial value and a LFSR characteristic polynomial for generating a pseudo-random number beforehand determined based on ID information being made from LFSR12 in LFSR12In the LFSR initial value characteristic polynomial set part 24the control signal SELBUS which shows an initial value and a LFSR characteristic polynomial for generating a pseudo-random number determined based on ID information is outputted to LFSR25.
[0078]LFSR25 is provided with the following.
Shift register 30.
LFSR feedback equivalent logic formation part 31.

[0079]Drawing 5 (a) shows an example of composition of the shift register 30 and the LFSR feedback equivalent logic formation part 31.
[0080]An initial value for generating a pseudo-random number determined by the LFSR initial value characteristic polynomial set part 24 is set as the shift register 30 as an initial value of data of N bit held at the shift register 30.
[0081]The LFSR feedback equivalent logic formation part 31 has two or more gate elements 33 for LFSR feedback equivalent logic formation for forming a logic synthesis gate equivalent to a LFSR characteristic polynomial. Each of two or more gate elements 33 for LFSR feedback equivalent logic formation is provided with the following.
Input terminal A.
Input terminal B.
Output terminal Y.
Select signal input terminal S.

[0082]Drawing 5 (b) shows an example of composition of the gate element 33 for LFSR feedback equivalent logic formation. The gate element 33 for LFSR feedback equivalent logic formation is provided with the following.
EOR arithmetic element 34.
The 4-1 selector 35.

[0083]The 4-1 selector 35 chooses one of four input signals according to a select

signal inputted into the select signal input terminal S. Four input signals are a signal which shows a result of having performed an EOR operation by the EOR arithmetic element 34 to a signal inputted from the input terminal Aa signal inputted from the input terminal Ba signal inputted from the input terminal Aand a signal inputted from the input terminal Band a signal which shows the logic phi. A signal with the 4-1 selected selector 35 is outputted from the output terminal Y.
[0084]A select signal is a part of control signal SELBUS outputted from the LFSR initial value characteristic polynomial set part 24. A select signal is based on a LFSR characteristic polynomial determined by the LFSR initial value characteristic polynomial set part 24.
[0085]Again with reference to drawing 5 (a)the LFSR feedback equivalent logic formation part 31 contains two or more gate elements 33 for LFSR feedback equivalent logic formation arranged by two or more pyramid type hierarchies. The N/2 gate elements 33 for LFSR feedback equivalent logic formation are located in a line with two or more of the hierarchies' least significant layer in parallelAn output from the output terminal Y of the two adjoining gate elements 33 for LFSR feedback equivalent logic formation is inputted into the input terminal A and the input terminal B of the gate element 33 for LFSR feedback equivalent logic formation of the upper layer.
[0086]The LFSR feedback equivalent logic formation part 31 sets an initial value for generating a pseudo-random number determined by the LFSR initial value characteristic polynomial set part 24 synchronizing with an initial value load signal supplied from the code generation controller 23 as the shift register 30.
[0087]The shift register 30 comprises N D flip-flops (DFF) 32 with set-reset connected in series.
[0088]If a shift clock is inputted into the shift register 301 bit of data of N bit currently held at the shift register 30 will be shifted in the direction of every predetermined one by one. For examplea bit currently held DFF32 of eye watch (K+1) is shifted to DFF32 of eye watch (K+2) at the same time a bit currently held the Kth DFF32 is shifted to DFF32 of eye watch (K+1) synchronizing with a shift clock. Thussynchronizing with a shift clockall the bits of data held at the shift register 30 are shifted simultaneously.
[0089]Each of output signal SOUT (1) - (N) outputted from N DFF32 is inputted into the gate element 33 for LFSR feedback equivalent logic formation arranged at a least significant layer of the LFSR feedback equivalent logic formation part 31. For examplethe output signal SOUT (1) and (2) is inputted into the input terminal A and the input terminal B of the gate element 33 for LFSR feedback equivalent logic formationrespectively. According to a select signal inputted into the select signal input terminal S of the gate element 33 for LFSR feedback equivalent logic formationone of four signals inputted into the 4-1 selector 35 is chosen. A selected signal is outputted from the output terminal Y of the gate element 33 for LFSR feedback equivalent logic formation. A signal outputted from the output terminal Y of the gate element 33 for LFSR feedback equivalent logic formation is inputted into the input terminal A or the input terminal B of the gate element 33

for LFSR feedback equivalent logic formation of the upper layer. Such processing is repeated toward a top layer of the LFSR feedback equivalent logic formation part 31. As a result1 bit is outputted from the one gate element 33 for LFSR feedback equivalent logic formation of a top layer. This value of 1 bit is fed back to an input of the 1st bit (namelythe 1st step of DFF32) of the data of N bit held at the shift register 30 as the control signal FBIN.

[0090]Synchronizing with a shift clock with which the shift register 30 is supplied from the code generation controller 23only the number of operation times M set up at random repeats shift operation and an EOR operation of the shift register 30. Data of N bit outputted from N DFF32 contained in the shift register 30 is outputted from LFSR25 as output data SOUT after an end of repetition processing. Output data SOUT expresses a pseudo-random number.

[0091]A shift clock inputted into the shift register 30 is the same signal as a shift clock inputted into LFSR12.

[0092]ThusLFSR25 generates a pseudo-random number equivalent to a pseudo-random number generated by LFSR12 according to a logical operation equivalent to a logical operation in LFSR12.

[0093]The number of times M of shift operation carried out in order to generate pseudorandom numbers in LFSR25 and LFSR12 is set up at random by the code generation controller 23. The number of times M of shift operation is set up based on time clocked by a timerfor example.

[0094]Again with reference to drawing 4the register (Key_Reg) 27 is connected to LFSR25 so that bit order of output data SOUT outputted from LFSR25 may be rearranged into predetermined bit order. Data of N bit held Key_Reg27 is considered as encryption / decryption KEY.

[0095]Bit width of output data SOUT and bit width of Key_Reg27 which are outputted from LFSR25 are the same as the larger one among bit width of data inputted into bit width and the treating part 21 of an address which are outputted from the treating part 21or it has become more than it. Thereforedata of a bit chosen among data of N bit held Key_Reg27 according to bit width of an address or bit width of data may be considered as encryption / decryption KEY.

[0096]A KEY reset signal and a KEY set clock are supplied to Key_Reg27 from the code generation controller 23. Synchronizing with a KEY reset signalthe encryption / decryption KEY currently held Key_Reg27 are reset. Synchronizing with a KEY set clockoutput data SOUT outputted from LFSR25 is incorporated into Key_Reg27and is held.

[0097]A KEY set clock inputted into Key_Reg27 is the same signal as a KEY set clock inputted into Key_Reg14.

[0098]ThusID_Reg36 and the LFSR initial value characteristic polynomial set part 24 function as a set part which sets up an initial value and a logical operation based on ID information peculiar to the memory storage 1. LFSR25 and Key_Reg27 function by performing a logical operation set up to a set-up initial value as an encryption/decryption KEY generation part which generates encryption / decryption KEY.

[0099]The encryption / decryption KEY held Key_Reg27 are given to the decryption EOR gate sequence 28 and the encryption EOR gate sequence 29.
[0100]The decryption EOR gate sequence 28 receives enciphered data from the memory storage 1Enciphered data is decrypted by receiving encryption / decryption KEY from Key_Reg27and performing an EOR operation to each bit of data and each bit of encryption / decryption KEY which were enciphered.
[0101]Thusthe decryption EOR gate sequence 28 functions as a decoding section which decrypts data enciphered based on encryption / decryption KEY.
[0102]The encryption EOR gate sequence 29 receives an address outputted from the treating part 21An address outputted from the treating part 21 is enciphered by receiving encryption / decryption KEY from Key_Reg27and performing an EOR operation to each bit of an address and each bit of encryption / decryption KEY which were outputted from the treating part 21.
[0103]Thusthe encryption EOR gate sequence 29 functions as an encryption section which enciphers an address outputted from the treating part 21 based on encryption / decryption KEY.
[0104]Nextwith reference to drawing 6operation of the data transfer system 100 containing the memory storage 1 and the data processing device 2 is explained.
[0105]Hard reset will be performed if the data processing device 2 is equipped with the memory storage 1. This hard reset is answered and the code generation controller 23 of the control section 20 is outputted to Key_Reg27 in which a "KEY reset signal" was formed by encryption/decryption machine 22and Key_Reg14 which were provided in encryption/decryption machine 11 (drawing 6 (b)). As a resultdata held Key_Reg14 and Key_Reg27 is reset by "ALL0"respectively (drawing 6 (a)). It is shown that it is in a state where encryption / decryption KEY was reset that data held Key_Reg14 and Key_Reg27 is "ALL0."
[0106]If "ALL0" is held Key_Reg14the selector 16 will output "the 0th address" to the storage parts store 10 irrespective of an address outputted from the decryption EOR gate sequence 15.
[0107]The storage parts store 10 outputs ID information memorized to "the 0th address." ID information is transmitted to the data processing device 2 via the encryption EOR gate sequence 17.
[0108]Thusin the state where encryption / decryption KEY was resetthere is no possibility that data may be read from addresses "other than 0th" by associating "the 0th street" of the state where encryption / decryption KEY was resetand the storage parts store 10. [of the storage parts store 10]
[0109]The code generation controller 23 of the control section 20 outputs "ID set signal" to ID_Reg36 (drawing 6 (i)). as a resultID information transmitted to the data processing device 2 from the memory storage 1 sets to ID_Reg36 -- having (drawing 6 (h)) -- it is outputted to the LFSR initial value characteristic polynomial set part 24.
[0110]The LFSR initial value characteristic polynomial set part 24 determines an initial value and a LFSR characteristic polynomial for generating a pseudo-random number based on ID information (drawing 6 (g)). The LFSR initial value

characteristic polynomial set part 24 outputs the control signal SELBUS for setting up an initial value and a LFSR characteristic polynomial for generating a pseudo-random number to the LFSR feedback equivalent logic formation part 31.
[0111]The code generation controller 23 of the control section 20 outputs an "initial value load signal" to LFSR12 and LFSR25 (drawing 6 (e)).
[0112]An "initial value load signal" is answeredan initial value is set as the shift register 18a of LFSR12and an initial value is set as the shift register 30 of LFSR25 (drawing 6 (d)). An initial value set as the shift register 18a is a value beforehand set up based on ID information hereand an initial value set as the shift register 30 is a value determined by the LFSR initial value characteristic polynomial set part 24 by an operation based on ID information.
[0113]The code generation controller 23 of the control section 20 outputs a "shift clock" to LFSR12 and LFSR25 (drawing 6 (f)).
[0114]A "shift clock" is answeredshift operation of an M_1 time is performed to the shift register 18a of LFSR12and shift operation of an M_1 time is performed to the shift register 30 of LFSR25 (drawing 6 (d)).
[0115]In LFSR12a logical operation based on [whenever it performs one shift operation] a LFSR specific polynomial is performed. The LFSR characteristic polynomial is a polynomial beforehand set up based on ID information. The logical operation result is fed back to an input of the shift register 18a. Similarlyin LFSR25a logical operation based on [whenever it performs one shift operation] a LFSR specific polynomial is performed. The LFSR characteristic polynomial is a polynomial determined by the LFSR initial value characteristic polynomial set part 24 by an operation based on ID information. The logical operation result is fed back to an input of the shift register 30.
[0116]Thusin LFSR12 and 25whenever a "shift clock" is inputtedshift operation and a logical operation are repeated. As a resultin encryption/decryption machines 11 and 22the same operation is completely performed.
[0117]Thusa circuit for realizing an initial value and a LFSR characteristic polynomial for generating a pseudo-random number beforehand determined based on ID information is beforehand included in LFSR12. Structure which can form LFSR12 and equivalent logic is beforehand prepared for LFSR25and based on ID information transmitted from the memory storage 1the LFSR initial value characteristic polynomial set part 24 constitutes LFSR25 so that LFSR12 and equivalent logic may be formed.
[0118]As a resultit is generated according to logic with equivalent the encryption / decryption KEY in encryption/decryption machine 11and the encryption/decryption KEY in encryption/decryption machine 22.
[0119]The code generation controller 23 of the control section 20 outputs a "KEY set clock" to Key_Reg14 and Key_Reg27after only the predetermined number of times outputs a "shift clock" to LFSR12 and LFSR25 (drawing 6 (c)).
[0120]While answering a "KEY set clock"incorporating into Key_Reg14 the output data OUT outputted from LFSR12 and being held thereoutput data SOUT outputted from LFSR25 is incorporated into Key_Reg27and is held there.

[0121]Thussame encryption / decryption KEY (for exampleA_1") will be held Key_Reg14 and Key_Reg27 (drawing 6 (a)).
[0122]When the data processing device 2 is equipped with the memory storage 1encryption/decryption machine 11 and encryption/decryption machine 22 are connected via a data bus and an address bus. Data enciphered based on encryption / decryption KEY is transmitted to the data processing device 2 from the memory storage 1 via a data bus (drawing 6 (j)). An address enciphered based on encryption / decryption KEY is transmitted to the memory storage 1 from the data processing device 2 via an address bus (drawing 6 (k)).
[0123]Thenthe treating part 21 outputs an address which specifies data which should be processed by the data processing device 2 among data memorized by the memory storage 1. The address is given to the encryption EOR gate sequence 29 of encryption/decryption machine 22.
[0124]The encryption EOR gate sequence 29 enciphers an address by performing an EOR operation to each bit of an addressand each bit of the encryption / decryption KEY currently held Key_Reg27. Specificallylogic (1/0) of a bit of an address corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed.An enciphered address is given to the decryption EOR gate sequence 15 of encryption/decryption machine 11.
[0125]The decryption EOR gate sequence 15 decrypts an enciphered address by performing an EOR operation to each bit of an enciphered addressand each bit of the encryption / decryption KEY currently held Key_Reg14. Specificallylogic (1/0) of a bit of an enciphered address corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed.
[0126]The encryption / decryption KEY currently held Key_Reg14and the encryption/decryption KEY currently held Key_Reg27 are the same. Thereforean enciphered address is changed into the original address by decrypting an address enciphered in a mode mentioned above.
[0127]An address outputted from the decryption EOR gate sequence 15 is given to the selector 16. The selector 16 judges whether it is in a state where encryption / decryption KEY is reset. When data currently held Key_Reg14 is except "ALL0"it judges with the selector 16 not being in a state where encryption / decryption KEY is reset. In this casethe selector 16 outputs an address outputted from the decryption EOR gate sequence 15 to the storage parts store 10.
[0128]The storage parts store 10 reads data memorized by position corresponding to an addressand outputs read data to the encryption EOR gate sequence 17.
[0129]The encryption EOR gate sequence 17 enciphers data outputted from the storage parts store 10 by performing an EOR operation to each bit of data outputted from the storage parts store 10and each bit of the encryption / decryption KEY currently held Key_Reg14. Specificallylogic (1/0) of a bit of data corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed. A principle of encryption by the encryption EOR gate sequence 17 is the same as a principle of encryption by the encryption EOR gate sequence 29.

Enciphered data is given to the decryption EOR gate sequence 28 of encryption/decryption machine 22.
[0130]The decryption EOR gate sequence 28 decrypts enciphered data by performing an EOR operation to each bit of enciphered dataand each bit of the encryption / decryption KEY currently held Key_Reg27. Specificallylogic (1/0) of a bit of enciphered data corresponding to a bit of two or more bits "1" of encryption / decryption KEY is reversed. A principle of decryption by the decryption EOR gate sequence 28 is the same as a principle of decryption by the decryption EOR gate sequence 15. Data outputted from the decryption EOR gate sequence 28 is given to the treating part 21.
[0131]The treating part 21 carries out predetermined processing to data outputted from the decryption EOR gate sequence 28.
[0132]Henceforthan operation for generating new encryption / decryption KEY in parallel to a data transfer between the memory storage 1 and the data processing device 2 is performed in LFSR12 and LFSR25. Such an operation may be performed for every fixed timeand may be performed for every random time.
[0133]The number of times (for exampleM_2 time) of shift operation made in LFSR12 and LFSR25 in order to generate new encryption / decryption KEYIt is set up differ from the number of times (for exampleM_1 time) of shift operation made in LFSR12 and LFSR25 in order to generate last encryption / decryption KEY (drawing 6 (d)).
[0134]A "KEY set clock" is answered and the encryption / decryption KEY currently held Key_Reg14 and Key_Reg27 are updated (drawing 6 (a)). Thendata enciphered as an address enciphered based on new encryption / decryption KEY is transmitted between the memory storage 1 and the data processing device 2 (drawing 6 (j)drawing 6 (k)).
[0135]Thusthe encryption / decryption KEY held Key_Reg14 of encryption/decryption machine 11and the encryption/decryption KEY held Key_Reg27 of encryption/decryption machine 22 answer a "KEY set clock"Simultaneous moreoverit is updated by momentary and new encryption / decryption KEY. Thereforealso when rewriting encryption / decryption KEYit is not necessary to interrupt data transfer and data transfer can be continuously carried out between the memory storage 1 and the data processing device 2.
[0136]this invention may be boiled not only in an above-mentioned embodiment but variouslyand may be changed. Although all the addresses and data other than ID information are enciphered and transmitted in the above-mentioned embodimentIn order to avoid unusual operation of a system when the inaccurate memory storage 1 is connected to the data processing device 2at the time of data requestssuch as a fundamental program areait may not be made not to perform an address and a data encryption.
[0137]Although the data processing device 2 was the composition that only the one memory storage 1 was connected and data was processedin the above-mentioned embodimentIt may encipher / be made to decrypt only data transmitted among the one memory storage 1 which connection of two or more memory

storage 1 was simultaneously possibleand was chosen from two or more memory storage 1 to the data processing device 2.
[0138]Although he is trying to memorize peculiar ID information to the memory storage 1 in the above-mentioned embodiment to "the 0th address" of the storage parts store 10 of the memory storage 1it may be made to provide a portion which stores ID information in addition to storage parts store 10 of the memory storage 1.
[0139]ID information peculiar to the memory storage 1 may be what kind of thingas long as it is usable for setting up not only ID numberssuch as a lot numberbut an initial value and a characteristic polynomial of LFSR.
[0140]
[Effect of the Invention]According to the data transfer system of this inventionthe address and data which are transmitted between memory storage and a data processing device are enciphered. For this reasonit is not easy to get to know the contents of the data memorized by memory storage from data transmitting. The data memorized by memory storage can be prevented from being reproduced unjustly by this.
[0141]According to the data transfer system of this inventionthe encryption / decryption KEY used for encryption and decryption of data transmitting are generated so that it may correspond to the ID information of the memory storage with which the data processing device was equipped. For this reasoneven if the data memorized by memory storage is reproduced as it isEncryption / decryption KEY is generated based on the ID information of memory storageand unless the structure which enciphers data based on encryption / decryption KEY is addedthe data processing device cannot read the duplication data correctly. It can prevent that duplicate use of the data memorized by memory storage is carried out unjustly by this.
[0142]The initial value and characteristic polynomial for generating encryption / decryption KEY based on ID information are beforehand made as a circuit by memory storage. Therebythe circuit for generating an initial value and a characteristic polynomialetc. become unnecessary. As a resultsmall-scale-ization of memory storage is realizable.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the example of composition of the data transfer system 100 of an embodiment of the invention.
[Drawing 2]It is a figure showing the example of composition of encryption/decryption machine 11 of the memory storage 1.
[Drawing 3]It is a figure showing the example of composition of LFSR12.
[Drawing 4]It is a figure showing the example of composition of encryption/decryption machine 22 of the data processing device 2.

[Drawing 5]The figure in which (a) shows the example of composition of the shift register 30 and the LFSR feedback equivalent logic formation part 31and (b) are the figures showing the example of composition of the gate element 33 for LFSR feedback equivalent logic formation.
[Drawing 6]It is a timing chart explaining operation of the data transfer system 100.
[Description of Notations]
1 Memory storage
2 Data processing device
10 Storage parts store
11 Encryption/decryption machine
12 LFSR
14 Key_Reg
15 Decryption EOR gate sequence
16 Selector
17 Encryption EOR gate sequence
20 Control section
21 Treating part
22 Encryption/decryption machine
23 Code generation controller
24 LFSR initial value characteristic polynomial set part
25 LFSR
27 Key_Reg
28 Decryption EOR gate sequence
29 Encryption EOR gate sequence
30 Shift register
31 LFSR feedback equivalent logic formation part
32 A D flip-flop with set-reset
33 The gate element for LFSR feedback equivalent logic formation
34 EOR arithmetic element
35 4-1 selector
36 ID_Reg

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－91828
（P2002－91828A）
(43)公開日　平成14年３月29日(2002.3.29)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G06F	12/14	320	G06F	12/14	320E　5B017
	1/00		G09C	1/00	650B　5B076
G09C	1/00	650			660D　5D044
		660	G11B	20/10	H　5J104
G11B	20/10		G06F	9/06	660L

審査請求　未請求　請求項の数19　ＯＬ　（全 15 頁）

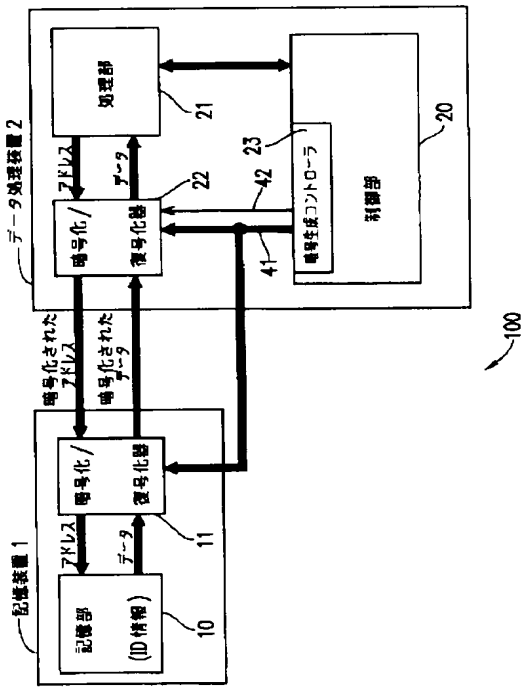
(21)出願番号　特願2000－282720(P2000－282720)
(22)出願日　平成12年９月18日(2000.9.18)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　河　範昭
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100078282
弁理士　山本　秀策

Ｆターム(参考)　5B017 AA06 BA07 CA14
5B076 FA05 FA10
5D044 AB02 AB05 AB07 BC08 CC08
DE50 GK17 HL08
5J104 AA01 AA07 AA16 EA04 EA26
KA04 NA02 NA05 NA41 PA14

(54)【発明の名称】　データ処理装置および記憶装置、並びに、それらを使用したデータ転送システム

(57)【要約】
【課題】　記憶装置に記憶されているデータが不正に複製されることを確実に防止する。
【解決手段】　データ処理装置２は、記憶装置１に記憶されたデータのうちデータ処理装置２によって処理されるべきデータを指定するアドレスを出力する処理部２１と、処理部２１から出力されたアドレスを暗号化し、暗号化されたアドレスを記憶装置１に送り、記憶装置１から暗号化されたデータを受け取り、暗号化されたデータを復号化する暗号化／復号化器２２とを備えている。暗号化／復号化器２２は、記憶装置１から記憶装置１に固有のＩＤ情報を受け取り、ＩＤ情報に基づいて初期値と論理演算とを設定する設定部（３６、２４）と、設定された初期値に対して設定された論理演算を行うことにより、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部（２５、２７）と、暗号化／復号化ＫＥＹに基づいてアドレスを暗号化する暗号化部２９と、暗号化／復号化ＫＥＹに基づいて暗号化されたデータを復号化する復号化部２８とを含む。



【特許請求の範囲】

【請求項１】　記憶装置を着脱可能なデータ処理装置であって、
前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、
前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する暗号化／復号化器とを備え、
前記暗号化／復号化器は、
前記記憶装置から前記記憶装置に固有のＩＤ情報を受け取り、前記ＩＤ情報に基づいて初期値と論理演算とを設定する設定部と、
前記設定された初期値に対して前記設定された論理演算を行うことにより、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部と、
前記暗号化／復号化ＫＥＹに基づいて前記アドレスを暗号化する暗号化部と、
前記暗号化／復号化ＫＥＹに基づいて前記暗号化されたデータを復号化する復号化部とを含む、データ処理装置。

【請求項２】　前記設定部は、前記記憶装置が前記データ処理装置に装着された際に、前記ＩＤ情報を暗号化されていない状態で受け取る、請求項１に記載のデータ処理装置。

【請求項３】　前記暗号化／復号化ＫＥＹ生成部は、定期的または不定期的に前記暗号化／復号化ＫＥＹを更新する、請求項１に記載のデータ処理装置。

【請求項４】　前記暗号化部は、前記暗号化／復号化ＫＥＹと前記アドレスとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記アドレスを暗号化し、
前記復号化部は、前記暗号化／復号化ＫＥＹと前記暗号化されたデータとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記暗号化されたデータを復号化する、請求項１に記載のデータ処理装置。

【請求項５】　前記暗号化／復号化ＫＥＹ生成部は、
複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、
前記シフトレジスタに保持されている前記データに対して前記設定された論理演算に応じた選択的な排他的論理和（ＥＯＲ）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック等価論理形成部とを含む、請求項１に記載のデータ処理装置。

【請求項６】　前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化ＫＥＹを生成する、請求項５に記載のデータ処理装置。

【請求項７】　前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化ＫＥＹを生成する、請求項５に記載のデータ処理装置。

【請求項８】　データ処理装置に脱着可能な記憶装置であって、
データが記憶された記憶部であって、アドレスに対応するデータを出力する記憶部と、
前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る暗号化／復号化器とを備え、
前記暗号化／復号化器は、
前記記憶装置に予め設定されている前記記憶装置に固有のＩＤ情報に基づいて、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部と、
前記暗号化／復号化ＫＥＹに基づいて前記暗号化されたアドレスを復号化する復号化部と、
前記暗号化／復号化ＫＥＹに基づいて前記記憶装置から出力された前記データを暗号化する暗号化部とを含む、記憶装置。

【請求項９】　前記暗号化／復号化ＫＥＹ生成部は、定期的または不定期的に前記暗号化／復号化ＫＥＹを更新する、請求項８に記載の記憶装置。

【請求項１０】　前記復号化部は、前記暗号化／復号化ＫＥＹと前記暗号化されたアドレスとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記暗号化されたアドレスを復号化し、
前記暗号化部は、前記暗号化／復号化ＫＥＹと前記データとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記データを暗号化する、請求項８に記載の記憶装置。

【請求項１１】　前記暗号化／復号化ＫＥＹ生成部は、
複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、
前記シフトレジスタに保持されている前記データに対して前記ＩＤ情報に基づき予め設定されている選択的な排他的論理和（ＥＯＲ）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック部とを含む、請求項８に記載の記憶装置。

【請求項１２】　前記シフトレジスタに保持されている前記データは、前記ＩＤ情報に基づき予め設定されている初期値に初期化されている、請求項１１に記載の記憶装置。

【請求項１３】　前記暗号化／復号化ＫＥＹ生成部は、
前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化ＫＥＹを生成する、請求項１１に記載の記憶装置。

【請求項１４】　前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化ＫＥＹを生成する、請求項１１に記載の記憶装置。
【請求項１５】　前記記憶部と前記暗号化／復号化器とは、単一の半導体チップ上に形成されている、請求項８に記載の記憶装置。
【請求項１６】　データ処理装置と、前記データ処理装置に着脱可能な記憶装置とを備えたデータ転送システムであって、
前記データ処理装置は、
前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、
前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する第１の暗号化／復号化器とを備え、
前記第１の暗号化／復号化器は、
前記記憶装置から前記記憶装置に固有のＩＤ情報を受け取り、前記ＩＤ情報に基づいて初期値と論理演算とを設定する設定部と、
前記設定された初期値に対して前記設定された論理演算を行うことにより、第１の暗号化／復号化ＫＥＹを生成する第１の暗号化／復号化ＫＥＹ生成部と、
前記第１の暗号化／復号化ＫＥＹに基づいて前記アドレスを暗号化する第１の暗号化部と、
前記第１の暗号化／復号化ＫＥＹに基づいて前記暗号化されたデータを復号化する第１の復号化部とを含み、
前記記憶装置は、
データが記憶された記憶部であって、前記アドレスに対応するデータを出力する記憶部と、
前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る第２の暗号化／復号化器とを備え、
前記第２の暗号化／復号化器は、
前記記憶装置に予め設定されている前記記憶装置に固有のＩＤ情報に基づいて、第２の暗号化／復号化ＫＥＹを生成する第２の暗号化／復号化ＫＥＹ生成部と、
前記第２の暗号化／復号化ＫＥＹに基づいて前記暗号化されたアドレスを復号化する第２の復号化部と、
前記第２の暗号化／復号化ＫＥＹに基づいて前記記憶装置から出力された前記データを暗号化する第２の暗号化部とを含む、データ転送システム。
【請求項１７】　前記第１の暗号化／復号化ＫＥＹと、前記第２の暗号化／復号化ＫＥＹとは、同等の論理に従って生成される、請求項１６に記載のデータ転送システム。
【請求項１８】　前記データ処理装置は、前記第１の暗号化／復号化器と前記第２の暗号化／復号化器とを少なくとも制御する制御部をさらに備えている、請求項１６に記載のデータ転送システム。
【請求項１９】　前記制御部は、前記記憶装置が前記データ処理装置に装着された際に、前記第１の暗号化／復号化ＫＥＹと前記第２の暗号化／復号化ＫＥＹとをリセットし、前記ＩＤ情報に基づいて同一の前記第１の暗号化／復号化ＫＥＹと前記第２の暗号化／復号化ＫＥＹとが生成されるように、前記第１の暗号化／復号化器と前記第２の暗号化／復号化器とを制御する、請求項１８に記載のデータ転送システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データ処理装置に着脱可能な記憶装置に記憶されているプログラムやデータが不正に複製されることを防止するデータ処理装置および記憶装置、並びに、データ伝送システムに関する。
【０００２】
【従来の技術】データ処理装置から取り外し可能な半導体記憶装置（例えば、ＲＯＭ）は、今日、家庭用ビデオゲームカセットなどの形で大量に市場に供給されている。もし不正複製防止対策を講じないとすると、ゲームカセットの海賊版が大量に市場に出回るおそれがある。
【０００３】従来、半導体記憶装置に記憶されているデータが不正に複製されることを防止する方法、あるいは、不正に複製されたデータを使用不能もしくは困難にする方法として、（１）暗号化されたデータを半導体記憶装置に記憶する方法、（２）半導体記憶装置に記憶されているデータを読み出す前に、半導体記憶装置もしくはデータ処理装置が正規のものであることを確認する認証手続きを行う方法が知られている。
【０００４】例えば、特開昭６０－１６７０３３号公報、特開昭６１－６７１３６号公報、特開平５－５３９２１号公報は、暗号化されたデータを半導体記憶装置に記憶する方法を開示している。
【０００５】また、例えば、特開平６－１６８１８５号公報、特許第２６９８３７１号公報は、半導体記憶装置が装着されるデータ処理装置が正規のものであることを確認する認証手続きを行った後に、半導体記憶装置に記憶されたデータを読み出す方法を開示している。
【０００６】
【発明が解決しようとする課題】暗号化されたデータを半導体記憶装置に記憶する方法では、半導体記憶装置に記憶されたデータそのものが暗号化されているために、半導体記憶装置から読み出されたデータの改変使用やプログラムの盗用を防止することができる。しかし、この方法では、半導体記憶装置に記憶されている暗号化されたデータが不正に複製されることを防止することはでき

ない。

【０００７】また、データ処理装置が正規のものであることを確認する認証手続きを行う方法では、正規でないデータ処理装置を用いて半導体記憶装置に記憶されているデータが不正に複製されることを防止することができる。しかし、この方法では、半導体記憶装置とデータ処理装置との間で転送される暗号化されていないデータを観測（プローブ）して読み取ることは可能であることから、半導体記憶装置に記憶されているデータ、プログラムの盗用を確実に防止することはできない。

【０００８】なお、無線情報通信等の開かれたネットワーク上の通信を暗号化する方法も知られている。例えば、特開平６－３４２２５７号公報、特開平８－３０７４１１号公報は、ＬＦＳＲ（リニア・フィードバック・シフト・レジスタ）を組み合わせて発生させた疑似乱数に基づいて暗号化／復号化ＫＥＹ（鍵）を生成し、この暗号化／復号化ＫＥＹ（鍵）に基づいて通信データを暗号化する方法を開示している。これらの公報に記載の暗号化技術は、秘密通信に関する技術である。これらの公報には、半導体記憶装置に記憶されているデータが不正に複製されることを防止することを目的としてそのような暗号化技術を使用することは示唆されていない。

【０００９】本発明は、上述した問題点を解決するためになされたものであり、データ処理装置に着脱可能な記憶装置に記憶されているプログラムやデータが不正に複製されることを防止するデータ処理装置および記憶装置、並びに、データ伝送システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明のデータ処理装置は、記憶装置を着脱可能なデータ処理装置であって、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のＩＤ情報を受け取り、前記ＩＤ情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部と、前記暗号化／復号化ＫＥＹに基づいて前記アドレスを暗号化する暗号化部と、前記暗号化／復号化ＫＥＹに基づいて前記暗号化されたデータを復号化する復号化部とを含み、これにより、上記目的が達成される。

【００１１】前記設定部は、前記記憶装置が前記データ処理装置に装着された際に、前記ＩＤ情報を暗号化されていない状態で受け取ってもよい。

【００１２】前記暗号化／復号化ＫＥＹ生成部は、定期的または不定期的に前記暗号化／復号化ＫＥＹを更新してもよい。

【００１３】前記暗号化部は、前記暗号化／復号化ＫＥＹと前記アドレスとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記アドレスを暗号化し、前記復号化部は、前記暗号化／復号化ＫＥＹと前記暗号化されたデータとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記暗号化されたデータを復号化してもよい。

【００１４】前記暗号化／復号化ＫＥＹ生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記設定された論理演算に応じた選択的な排他的論理和（ＥＯＲ）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック等価論理形成部とを含んでいてもよい。

【００１５】前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化ＫＥＹを生成してもよい。

【００１６】前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化ＫＥＹを生成してもよい。

【００１７】本発明の記憶装置は、データ処理装置に脱着可能な記憶装置であって、データが記憶された記憶部であって、アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る暗号化／復号化器とを備え、前記暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のＩＤ情報に基づいて、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部と、前記暗号化／復号化ＫＥＹに基づいて前記暗号化されたアドレスを復号化する復号化部と、前記暗号化／復号化ＫＥＹに基づいて前記記憶装置から出力された前記データを暗号化する暗号化部とを含み、これにより、上記目的が達成される。

【００１８】前記暗号化／復号化ＫＥＹ生成部は、定期的または不定期的に前記暗号化／復号化ＫＥＹを更新してもよい。

【００１９】前記復号化部は、前記暗号化／復号化ＫＥＹと前記暗号化されたアドレスとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記暗号化されたアドレスを復号化し、前記暗号化部は、前記暗号化／復号化ＫＥＹと前記データとに対して排他的論理和（ＥＯＲ）演算を行うことにより、前記データを暗号化しても

よい。

【００２０】前記暗号化／復号化ＫＥＹ生成部は、複数のビットを含むデータを保持し、シフトクロックに従って前記データをシフトさせるシフトレジスタと、前記シフトレジスタに保持されている前記データに対して前記ＩＤ情報に基づき予め設定されている選択的な排他的論理和（ＥＯＲ）演算を行い、その演算結果を前記シフトレジスタの入力にフィードバックするフィードバック部とを含んでいてもよい。

【００２１】前記シフトレジスタに保持されている前記データは、前記ＩＤ情報に基づき予め設定されている初期値に初期化されていてもよい。

【００２２】前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データのビット順序を所定の順序に並び替えることにより、前記暗号化／復号化ＫＥＹを生成してもよい。

【００２３】前記暗号化／復号化ＫＥＹ生成部は、前記シフトレジスタに保持されている前記データをシフトする回数を変更することにより、新たな暗号化／復号化ＫＥＹを生成してもよい。

【００２４】前記記憶部と前記暗号化／復号化器とは、単一の半導体チップ上に形成されていてもよい。

【００２５】本発明のデータ転送システムは、データ処理装置と、前記データ処理装置に着脱可能な記憶装置とを備えたデータ転送システムであって、前記データ処理装置は、前記記憶装置に記憶されたデータのうち前記データ処理装置によって処理されるべきデータを指定するアドレスを出力する処理部と、前記処理部から出力された前記アドレスを暗号化し、前記暗号化されたアドレスを前記記憶装置に送り、前記記憶装置から暗号化されたデータを受け取り、前記暗号化されたデータを復号化する第１の暗号化／復号化器とを備え、前記第１の暗号化／復号化器は、前記記憶装置から前記記憶装置に固有のＩＤ情報を受け取り、前記ＩＤ情報に基づいて初期値と論理演算とを設定する設定部と、前記設定された初期値に対して前記設定された論理演算を行うことにより、第１の暗号化／復号化ＫＥＹを生成する第１の暗号化／復号化ＫＥＹ生成部と、前記第１の暗号化／復号化ＫＥＹに基づいて前記アドレスを暗号化する第１の暗号化部と、前記第１の暗号化／復号化ＫＥＹに基づいて前記暗号化されたデータを復号化する第１の復号化部とを含み、前記記憶装置は、データが記憶された記憶部であって、前記アドレスに対応するデータを出力する記憶部と、前記データ処理装置から暗号化されたアドレスを受け取り、前記暗号化されたアドレスを復号化し、前記記憶装置から出力された前記データを暗号化し、前記暗号化されたデータを前記データ処理装置に送る第２の暗号化／復号化器とを備え、前記第２の暗号化／復号化器は、前記記憶装置に予め設定されている前記記憶装置に固有のＩＤ情報に基づいて、第２の暗号化／復号化ＫＥＹを生成する第２の暗号化／復号化ＫＥＹ生成部と、前記第２の暗号化／復号化ＫＥＹに基づいて前記暗号化されたアドレスを復号化する第２の復号化部と、前記第２の暗号化／復号化ＫＥＹに基づいて前記記憶装置から出力された前記データを暗号化する第２の暗号化部とを含み、これにより、上記目的が達成される。

【００２６】前記第１の暗号化／復号化ＫＥＹと、前記第２の暗号化／復号化ＫＥＹとは、同等の論理に従って生成されてもよい。

【００２７】前記データ処理装置は、前記第１の暗号化／復号化器と前記第２の暗号化／復号化器とを少なくとも制御する制御部をさらに備えていてもよい。

【００２８】前記制御部は、前記記憶装置が前記データ処理装置に装着された際に、前記第１の暗号化／復号化ＫＥＹと前記第２の暗号化／復号化ＫＥＹとをリセットし、前記ＩＤ情報に基づいて同一の前記第１の暗号化／復号化ＫＥＹと前記第２の暗号化／復号化ＫＥＹとが生成されるように、前記第１の暗号化／復号化器と前記第２の暗号化／復号化器とを制御してもよい。

【００２９】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を説明する。

【００３０】図１は、本発明の実施の形態のデータ転送システム１００の構成例を示す。

【００３１】データ転送システム１００は、記憶装置１と、データ処理装置２とを含む。記憶装置１は、データ処理装置２に着脱可能に構成されている。データ処理装置２には、同一規格の複数の記憶装置から選択される１つの記憶装置１が装着される。

【００３２】データ処理装置２は、装着された記憶装置１に暗号化されたアドレスを出力する。記憶装置１は、暗号化されたアドレスに対応する暗号化されたデータをデータ処理装置２に出力する。このように、記憶装置１とデータ処理装置２との間で転送されるアドレスおよびデータを暗号化することによって、転送データから記憶装置１に記憶されているデータの内容を知ることは困難になる。

【００３３】記憶装置１は、例えば、ゲームプログラムや各種データが記憶された家庭用ビデオゲーム用のゲームカセットである。データ処理装置２は、例えば、家庭用ビデオゲーム機である。家庭用ビデオゲーム機は、ゲームカセットを装着するための差し込み口を有している。ゲームカセットが家庭用ビデオゲーム機の差し込み口に装着されると、ゲームカセットに記憶されているゲームプログラムや各種データが家庭用ビデオゲーム機に読み出され、家庭用ビデオゲーム機に接続されているテレビなどのディスプレイにゲーム画面が表示される。

【００３４】記憶装置１は、記憶部１０と、暗号化／復号化器１１とを含む。記憶部１０と暗号化／復号化器１１とは、単一の半導体チップ（例えば、シリコンチッ

プ）上に形成されていることが好ましい。

【００３５】記憶部１０には、記憶装置１に固有のＩＤ情報（例えば、ＩＤ番号）と、プログラムや各種データとが予め記憶されている。ＩＤ情報は、例えば、同一規格の記憶装置（製品）毎に割り振られる品番である。あるいは、ＩＤ情報は、複数の値から選択された値であってもよい。ＩＤ情報は、記憶部１０の所定のアドレス（例えば、「０番地」）に記憶される。記憶部１０は、暗号化／復号化器１１からアドレスを受け取り、そのアドレスに対応する位置に記憶されているデータを暗号化／復号化器１１に出力する。

【００３６】なお、本明細書では、用語「データ」は、記憶部１０に記憶され得る任意のタイプの情報を意味するものとし、プログラムや各種データを含む包括的な用語として理解される。

【００３７】暗号化／復号化器１１は、暗号化されたアドレスをデータ処理装置２から受け取り、その暗号化されたアドレスを復号化することによりアドレスを生成する。そのアドレスは、記憶部１０に出力される。また、暗号化／復号化器１１は、記憶部１０から出力されたデータを受け取り、そのデータを暗号化することにより暗号化されたデータを生成する。その暗号化されたデータは、データ処理装置２に出力される。

【００３８】データ処理装置２は、処理部２１と、暗号化／復号化器２２とを含む。

【００３９】記憶装置１がデータ処理装置２に装着されると、記憶装置１内の暗号化／復号化器１１とデータ処理装置２内の暗号化／復号化器２２とは互いに電気的に接続された状態となる。例えば、暗号化／復号化器１１と暗号化／復号化器２２とはコネクタ（図示せず）を介して互いに電気的に接続され得る。

【００４０】処理部２１は、記憶装置１に記憶されているデータのうちデータ処理装置２によって処理されるべきデータを指定するアドレスを出力する。

【００４１】暗号化／復号化器２２は、処理部２１から出力されたアドレスを受け取り、そのアドレスを暗号化することにより暗号化されたアドレスを生成する。その暗号化されたアドレスは、記憶装置１に出力される。また、暗号化／復号化器２２は、記憶装置１から出力された暗号化されたデータを受け取り、その暗号化されたデータを復号化することによりデータを生成する。そのデータは、処理部２１に出力される。

【００４２】データ処理装置２は、暗号化／復号化器１１と暗号化／復号化器２２と処理部２１とを制御する制御部２０をさらに含んでいる。

【００４３】制御部２０は、暗号生成コントローラ２３を含む。暗号生成コントローラ２３は、暗号化／復号化器１１における暗号化／復号化ＫＥＹの生成および変更のタイミングと暗号化／復号化器２２における暗号化／復号化ＫＥＹの生成および変更のタイミングとが同期するように、暗号化／復号化器１１および暗号化／復号化器２２を制御する。

【００４４】暗号生成コントローラ２３は、暗号化／復号化器１１および暗号化／復号化器２２に共通の制御信号を制御信号線４１を介して暗号化／復号化器１１および暗号化／復号化器２２に供給し、暗号化／復号化器２２のみに関連する制御信号を制御信号線４２を介して暗号化／復号化器２２に供給する。

【００４５】図２は、記憶装置１の暗号化／復号化器１１の構成例を示す。

【００４６】暗号化／復号化器１１は、疑似乱数を生成するＬＦＳＲ（Ｌｉｎｅａｒ　Ｆｅｅｄｂａｃｋ　Ｓｈｉｆｔ　Ｒｅｇｉｓｔｅｒ）１２を含む。

【００４７】ＬＦＳＲ１２は、シフトレジスタに保持されているＮビットのデータのうち選択されたいくつかのビットに対して排他的論理和（Ｅｘｃｌｕｓｉｖｅ　ＯＲ；以下、「ＥＯＲ」という）演算を行い、その演算結果をシフトレジスタの入力にフィードバックする回路である。シフトレジスタは、例えば、Ｄフリップフロップ（ＤＦＦ）を直列に接続することによって構成される。

【００４８】シフトレジスタに保持されているＮビットのデータのうちいずれのビットに対してＥＯＲ演算を行い、その演算結果をシフトレジスタのいずれのビット位置にフィードバックするかにより、特性の異なる最大2^N-1の周期の擬似乱数（パターン）列を得ることができる。ここで、最大である2^N-1の周期を有する擬似乱数列は、一般に、「Ｍ系列（Ｍａｘｉｍａｍ　ｌｅｎｇｔｈ　Ｓｅｑｕｅｎｃｅｓ）」と呼ばれる。ここで、Ｎは２以上の任意の整数である。

【００４９】なお、シフトレジスタに保持されているＮビットのデータのうちいずれのビットに対してＥＯＲ演算を行うかは、（数１）に示されるＮ次の多項式によって表すことができる。

【００５０】

【数１】

$$f(x)=\sum_{k=0}^{n}a_k x^k \quad \cdots\cdots \quad (1)$$

ただし、シフトレジスタに保持されているＮビットのデータのうちｋ番目のビットをＥＯＲ演算に使用する場合は$a_k=1$、シフトレジスタに保持されているＮビットのデータのうちｋ番目のビットをＥＯＲ演算に使用しない場合は$a_k=0$とし、$a_0=1$および$a_N=1$とされる。この多項式ｆ（ｘ）は、ＬＦＳＲ特性多項式と呼ばれ、ＬＦＳＲが発生する擬似乱数の特性を表す。

【００５１】例えば、Ｎ＝４の場合において、１番目のビットおよび４番目のビットに対してＥＯＲ演算を行う場合には、ＬＦＳＲ特性多項式ｆ（ｘ）は、「x^4+x+1」と表される。

【００５２】Ｍ系列を形成するためのＬＦＳＲ特性多項

式は限られているが、本発明では、得られる擬似乱数列が特にM系列である必要はない。ただし、シフトレジスタに保持されるＮビットのデータの初期値として、この処理を繰り返してもシフトレジスタに保持されるＮビットのデータに変化が起こらないデッドループ（またはスタックステート）を起こすような値（例えば、「０・・・０（ＡＬＬ０）」）を設定することは避けなければならない。

【００５３】記憶部１０に記憶されているＩＤ情報に基づいて、ＬＦＳＲのシフトレジスタに保持されるべきＮビットのデータの初期値と、ＬＦＳＲ特性多項式とが予め決定される。ＬＦＳＲ１２は、その予め決定されたＮビットのデータの初期値とＬＦＳＲ特性多項式とを満たす回路として形成される。

【００５４】図３は、ＬＦＳＲ１２の構成例を示す。ＬＦＳＲ１２は、Ｎビットのデータを保持するシフトレジスタ１８ａを有している。シフトレジスタ１８ａは、直列に接続されたＮ個のＤフリップフロップ（ＤＦＦ）１８から構成されている。

【００５５】ＬＦＳＲ１２に初期値ロード信号が入力されると、シフトレジスタ１８ａに保持されているＮビットのデータが初期化される。そのＮビットのデータの初期値は、Ｎ個のレジスタ１９に予め記憶されている。そのＮビットのデータの初期値は、記憶部１０に記憶されているＩＤ情報に基づいて予め決定されている。あるいは、そのＮビットのデータの初期値は、Ｎ個のＤＦＦ１８の各ビットに入力される初期値ロード信号が各ビットの非同期セットあるいは非同期リセットのいずれかに接続されている事で予め決定されている。

【００５６】ＬＦＳＲ１２にシフトクロックが入力されると、シフトレジスタ１８ａに保持されているＮビットのデータは、順次、１ビットずつ所定の方向にシフトされる。シフト回数は、任意の回数に設定することが可能である。

【００５７】記憶部１０に記憶されているＩＤ情報に基づいて予め決定された選択規則に従って、シフトレジスタ１８ａに保持されているＮビットのデータのうちのいくつかのビットが選択され、選択されたビットに対してＥＯＲ演算が行われる。そのＥＯＲ演算の結果は、シフトレジスタ１８ａの１番目のビット（すなわち、１段目のＤＦＦ１８）の入力にフィードバックされる。図３に示される例では、シフトレジスタ１８ａに保持されているＮビットのデータのうち、１番目のビットと３番目のビットとに対してＥＯＲ演算が行われ、そのＥＯＲ演算の結果がシフトレジスタ１８ａの１番目のビットの入力にフィードバックされる。ＥＯＲ演算素子１３が、１番目のビットと３番目のビットとに対してＥＯＲ演算を行うために使用される。

【００５８】シフトレジスタ１８ａに保持されるＮビットのデータの初期値と、シフトレジスタ１８ａに保持されるＮビットのデータのうちのいずれのビットを選択してＥＯＲ演算を行うかを規定する選択規則とは、記憶部１０に記憶されているＩＤ情報に基づいて一義的に決定される。

【００５９】ＬＦＳＲ１２は、暗号生成コントローラ２３から供給されるシフトクロックに同期して、ランダムに設定される演算回数Ｍだけ、シフトレジスタ１８ａのシフト演算およびＥＯＲ演算を繰り返す。繰り返し処理の終了後、シフトレジスタ１８ａに含まれるＮ個のＤＦＦ１８から出力されるＮビットのデータが出力データＯＵＴとしてＬＦＳＲ１２から出力される。出力データＯＵＴは、疑似乱数を表す。

【００６０】図２を再び参照して、レジスタ（Ｋｅｙ＿Ｒｅｇ）１４は、ＬＦＳＲ１２から出力される出力データＯＵＴのビット順序を所定のビット順序に並び替えるようにＬＦＳＲ１２に接続されている。Ｋｅｙ＿Ｒｅｇ１４に保持されるＮビットのデータが、暗号化／復号化ＫＥＹとされる。

【００６１】なお、ＬＦＳＲ１２から出力される出力データＯＵＴのビット幅とＫｅｙ＿Ｒｅｇ１４のビット幅とは、記憶部１０に入力されるアドレスのビット幅および記憶部１０から出力されるデータのビット幅のうち大きい方と同じもしくはそれ以上となっている。従って、Ｋｅｙ＿Ｒｅｇ１４に保持されるＮビットのデータのうち、アドレスのビット幅またはデータのビット幅に応じて選択されたビットのデータが暗号化／復号化ＫＥＹとされ得る。

【００６２】Ｋｅｙ＿Ｒｅｇ１４には、暗号生成コントローラ２３からＫＥＹリセット信号およびＫＥＹセットクロックが供給される。ＫＥＹリセット信号に同期して、Ｋｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹがリセットされる。ＫＥＹセットクロックに同期して、ＬＦＳＲ１２から出力される出力データＯＵＴがＫｅｙ＿Ｒｅｇ１４に取り込まれ、保持される。

【００６３】ＫＥＹセットクロックは、暗号生成コントローラ２３から定期的または不定期的に出力される。暗号化／復号化ＫＥＹは、ＫＥＹセットクロックに応答して、定期的または不定期的に更新される。

【００６４】このように、ＬＦＳＲ１２およびＫｅｙ＿Ｒｅｇ１４は、記憶装置１に予め設定されている記憶装置１に固有のＩＤ情報に基づいて、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部として機能する。

【００６５】Ｋｅｙ＿Ｒｅｇ１４に保持される暗号化／復号化ＫＥＹは、復号化ＥＯＲゲート列１５と暗号化ＥＯＲゲート列１７とに与えられる。

【００６６】復号化ＥＯＲゲート列１５は、暗号化されたアドレスをデータ処理装置２から受け取り、暗号化／復号化ＫＥＹをＫｅｙ＿Ｒｅｇ１４から受け取り、暗号化されたアドレスの各ビットと暗号化／復号化ＫＥＹの

各ビットとに対してＥＯＲ演算を行うことにより、暗号化されたアドレスを復号化する。

【００６７】このように、復号化ＥＯＲゲート列１５は、暗号化／復号化ＫＥＹに基づいて暗号化されたアドレスを復号化する復号化部として機能する。

【００６８】復号化ＥＯＲゲート列１５によるＥＯＲ演算結果は、セレクタ１６に与えられる。セレクタ１６は、Ｋｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹを参照して、暗号化／復号化ＫＥＹが「ＡＬＬ０」（すべてのビットが「０」であり、暗号化／復号化ＫＥＹが設定されていない状態）である場合には、「０番地」のアドレスを記憶部１０に出力し、暗号化／復号化ＫＥＹが「ＡＬＬ０」でない場合には、復号化ＥＯＲゲート列１５から出力されるアドレスを記憶部１０に出力する。

【００６９】記憶部１０は、セレクタ１６から出力されるアドレスに対応する位置に格納されているデータを出力する。

【００７０】暗号化ＥＯＲゲート列１７は、記憶部１０から出力されたデータを受け取り、暗号化／復号化ＫＥＹをＫｅｙ＿Ｒｅｇ１４から受け取り、記憶部１０から出力されたデータの各ビットと暗号化／復号化ＫＥＹの各ビットとに対してＥＯＲ演算を行うことにより、記憶部１０から出力されたデータを暗号化する。

【００７１】このように、暗号化ＥＯＲゲート列１７は、暗号化／復号化ＫＥＹに基づいて記憶部１０から出力されたデータを暗号化する暗号化部として機能する。

【００７２】上述したように、Ｋｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹが「ＡＬＬ０」である場合には、セレクタ１６は、復号化ＥＯＲゲート列１５から出力されるアドレスにかかわらず、「０番地」のアドレスを記憶部１０に出力する。記憶部１０は、「０番地」のアドレスに対して「０番地」に記憶されているＩＤ情報を出力する。この場合、暗号化ＥＯＲゲート列１７は、「ＡＬＬ０」とＩＤ情報とに対してＥＯＲ演算を行うことになる。その結果、暗号化ＥＯＲゲート列１７からＩＤ情報が出力される。

【００７３】図４は、データ処理装置２の暗号化／復号化器２２の構成例を示す。

【００７４】暗号化／復号化器２２は、記憶装置１から出力されたＩＤ情報を保持するレジスタ（ＩＤ＿Ｒｅｇ）３６と、ＩＤ＿Ｒｅｇ３６に保持されたＩＤ情報に基づいて、疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを決定するＬＦＳＲ初期値特性多項式設定部２４とを含む。

【００７５】記憶装置１がデータ処理装置２に装着されると、記憶装置１からデータ処理装置２にＩＤ情報が転送される。このＩＤ情報は、暗号化されていない状態で転送される。

【００７６】ＩＤ＿Ｒｅｇ３６は、暗号生成コントローラ２３から供給されるＩＤセット信号に同期して、記憶装置１から転送されたＩＤ情報を取り込み、保持する。ＩＤ＿Ｒｅｇ３６に保持されたＩＤ情報は、ＬＦＳＲ初期値特性多項式設定部２４に出力される。

【００７７】ＬＦＳＲ初期値特性多項式設定部２４において、ＩＤ情報に基づいて疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを決定する際に使用される論理は、記憶装置１の暗号化／復号化器１１に設けられたＬＦＳＲ１２において、ＩＤ情報に基づいて疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを予め決定する際に使用された論理と同等である。ＬＦＳＲ１２では、ＩＤ情報に基づき予め決定された疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを実現する回路がＬＦＳＲ１２内に作り込まれているのに対し、ＬＦＳＲ初期値特性多項式設定部２４では、ＩＤ情報に基づき決定された疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを示す制御信号ＳＥＬＢＵＳがＬＦＳＲ２５に出力される。

【００７８】ＬＦＳＲ２５は、シフトレジスタ３０と、ＬＦＳＲフィードバック等価論理形成部３１とを含む。

【００７９】図５（ａ）は、シフトレジスタ３０およびＬＦＳＲフィードバック等価論理形成部３１の構成例を示す。

【００８０】ＬＦＳＲ初期値特性多項式設定部２４によって決定された疑似乱数を生成するための初期値は、シフトレジスタ３０に保持されるＮビットのデータの初期値としてシフトレジスタ３０に設定される。

【００８１】ＬＦＳＲフィードバック等価論理形成部３１は、ＬＦＳＲ特性多項式と等価な論理合成ゲートを形成するための複数のＬＦＳＲフィードバック等価論理形成用ゲート素子３３を有している。複数のＬＦＳＲフィードバック等価論理形成用ゲート素子３３のそれぞれは、入力端子Ａと、入力端子Ｂと、出力端子Ｙと、セレクト信号入力端子Ｓとを有している。

【００８２】図５（ｂ）は、ＬＦＳＲフィードバック等価論理形成用ゲート素子３３の構成例を示す。ＬＦＳＲフィードバック等価論理形成用ゲート素子３３は、ＥＯＲ演算素子３４と、４－１セレクタ３５とを含む。

【００８３】４－１セレクタ３５は、セレクト信号入力端子Ｓに入力されるセレクト信号に従って、４つの入力信号のうちの１つを選択する。４つの入力信号は、入力端子Ａから入力される信号、入力端子Ｂから入力される信号、入力端子Ａから入力される信号と入力端子Ｂから入力される信号とに対してＥＯＲ演算素子３４によるＥＯＲ演算を行った結果を示す信号、論理φを示す信号である。４－１セレクタ３５によって選択された信号は、出力端子Ｙから出力される。

【００８４】セレクト信号は、ＬＦＳＲ初期値特性多項式設定部２４から出力される制御信号ＳＥＬＢＵＳの一部である。セレクト信号は、ＬＦＳＲ初期値特性多項式

設定部２４によって決定されたＬＦＳＲ特性多項式に基づいている。

【００８５】図５（ａ）を再び参照して、ＬＦＳＲフィードバック等価論理形成部３１は、ピラミッド型の複数の階層に配列された複数のＬＦＳＲフィードバック等価論理形成用ゲート素子３３を含む。その複数の階層の最下位層には、Ｎ／２個のＬＦＳＲフィードバック等価論理形成用ゲート素子３３が並列に並び、隣接する２つのＬＦＳＲフィードバック等価論理形成用ゲート素子３３の出力端子Ｙからの出力が、上位層のＬＦＳＲフィードバック等価論理形成用ゲート素子３３の入力端子Ａおよび入力端子Ｂに入力される。

【００８６】ＬＦＳＲフィードバック等価論理形成部３１は、暗号生成コントローラ２３から供給される初期値ロード信号に同期して、ＬＦＳＲ初期値特性多項式設定部２４によって決定された疑似乱数を発生させるための初期値をシフトレジスタ３０に設定する。

【００８７】シフトレジスタ３０は、直列に接続されたＮ個のセットリセット付きＤフリップフロップ（ＤＦＦ）３２から構成されている。

【００８８】シフトレジスタ３０にシフトクロックが入力されると、シフトレジスタ３０に保持されているＮビットのデータは、順次、１ビットずつ所定の方向にシフトされる。例えば、シフトクロックに同期して、Ｋ番目のＤＦＦ３２に保持されていたビットは、（Ｋ＋１）番目のＤＦＦ３２にシフトされると同時に、（Ｋ＋１）番目のＤＦＦ３２に保持されていたビットは、（Ｋ＋２）番目のＤＦＦ３２にシフトされる。このように、シフトクロックに同期して、シフトレジスタ３０に保持されるデータのすべてのビットが同時にシフトされる。

【００８９】Ｎ個のＤＦＦ３２から出力される出力信号ＳＯＵＴ（１）～（Ｎ）のそれぞれは、ＬＦＳＲフィードバック等価論理形成部３１の最下位層に配置されているＬＦＳＲフィードバック等価論理形成用ゲート素子３３に入力される。例えば、出力信号ＳＯＵＴ（１）および（２）は、それぞれ、ＬＦＳＲフィードバック等価論理形成用ゲート素子３３の入力端子Ａおよび入力端子Ｂに入力される。そのＬＦＳＲフィードバック等価論理形成用ゲート素子３３のセレクト信号入力端子Ｓに入力されるセレクト信号に応じて、４－１セレクタ３５に入力される４つの信号のうちの１つの信号が選択される。選択された信号は、そのＬＦＳＲフィードバック等価論理形成用ゲート素子３３の出力端子Ｙから出力される。そのＬＦＳＲフィードバック等価論理形成用ゲート素子３３の出力端子Ｙから出力された信号は、上位層のＬＦＳＲフィードバック等価論理形成用ゲート素子３３の入力端子Ａまたは入力端子Ｂに入力される。このような処理が、ＬＦＳＲフィードバック等価論理形成部３１の最上位層に向かって繰り返される。その結果、最上位層の１つのＬＦＳＲフィードバック等価論理形成用ゲート素子３３から１ビットが出力される。この１ビットの値は、制御信号ＦＢＩＮとして、シフトレジスタ３０に保持されるＮビットのデータのうちの１番目のビット（すなわち、１段目のＤＦＦ３２）の入力にフィードバックされる。

【００９０】シフトレジスタ３０は、暗号生成コントローラ２３から供給されるシフトクロックに同期して、ランダムに設定される演算回数Ｍだけ、シフトレジスタ３０のシフト演算およびＥＯＲ演算を繰り返す。繰り返し処理の終了後、シフトレジスタ３０に含まれるＮ個のＤＦＦ３２から出力されるＮビットのデータが出力データＳＯＵＴとしてＬＦＳＲ２５から出力される。出力データＳＯＵＴは、疑似乱数を表す。

【００９１】なお、シフトレジスタ３０に入力されるシフトクロックは、ＬＦＳＲ１２に入力されるシフトクロックと同一の信号である。

【００９２】このように、ＬＦＳＲ２５は、ＬＦＳＲ１２における論理演算と同等の論理演算に従って、ＬＦＳＲ１２によって生成される疑似乱数と同等の疑似乱数を生成する。

【００９３】ＬＦＳＲ２５およびＬＦＳＲ１２において擬似乱数を生成するために実施されるシフト演算の回数Ｍは、暗号生成コントローラ２３によってランダムに設定される。シフト演算の回数Ｍは、例えば、タイマーによって計時される時間に基づいて設定される。

【００９４】図４を再び参照して、レジスタ（Ｋｅｙ＿Ｒｅｇ）２７は、ＬＦＳＲ２５から出力される出力データＳＯＵＴのビット順序を所定のビット順序に並び替えるようにＬＦＳＲ２５に接続されている。Ｋｅｙ＿Ｒｅｇ２７に保持されるＮビットのデータが、暗号化／復号化ＫＥＹとされる。

【００９５】なお、ＬＦＳＲ２５から出力される出力データＳＯＵＴのビット幅とＫｅｙ＿Ｒｅｇ２７のビット幅とは、処理部２１から出力されるアドレスのビット幅および処理部２１に入力されるデータのビット幅のうち大きい方と同じもしくはそれ以上となっている。従って、Ｋｅｙ＿Ｒｅｇ２７に保持されるＮビットのデータのうち、アドレスのビット幅またはデータのビット幅に応じて選択されたビットのデータが暗号化／復号化ＫＥＹとされ得る。

【００９６】Ｋｅｙ＿Ｒｅｇ２７には、暗号生成コントローラ２３からＫＥＹリセット信号およびＫＥＹセットクロックが供給される。ＫＥＹリセット信号に同期して、Ｋｅｙ＿Ｒｅｇ２７に保持されている暗号化／復号化ＫＥＹがリセットされる。ＫＥＹセットクロックに同期して、ＬＦＳＲ２５から出力される出力データＳＯＵＴがＫｅｙ＿Ｒｅｇ２７に取り込まれ、保持される。

【００９７】なお、Ｋｅｙ＿Ｒｅｇ２７に入力されるＫＥＹセットクロックは、Ｋｅｙ＿Ｒｅｇ１４に入力されるＫＥＹセットクロックと同一の信号である。

【００９８】このように、ＩＤ＿Ｒｅｇ３６およびＬＦＳＲ初期値特性多項式設定部２４は、記憶装置１に固有のＩＤ情報に基づいて、初期値と論理演算とを設定する設定部として機能する。また、ＬＦＳＲ２５およびＫｅｙ＿Ｒｅｇ２７は、設定された初期値に対して設定された論理演算を行うことにより、暗号化／復号化ＫＥＹを生成する暗号化／復号化ＫＥＹ生成部として機能する。

【００９９】Ｋｅｙ＿Ｒｅｇ２７に保持される暗号化／復号化ＫＥＹは、復号化ＥＯＲゲート列２８と暗号化ＥＯＲゲート列２９とに与えられる。

【０１００】復号化ＥＯＲゲート列２８は、暗号化されたデータを記憶装置１から受け取り、暗号化／復号化ＫＥＹをＫｅｙ＿Ｒｅｇ２７から受け取り、暗号化されたデータの各ビットと暗号化／復号化ＫＥＹの各ビットとに対してＥＯＲ演算を行うことにより、暗号化されたデータを復号化する。

【０１０１】このように、復号化ＥＯＲゲート列２８は、暗号化／復号化ＫＥＹに基づいて暗号化されたデータを復号化する復号化部として機能する。

【０１０２】暗号化ＥＯＲゲート列２９は、処理部２１から出力されたアドレスを受け取り、暗号化／復号化ＫＥＹをＫｅｙ＿Ｒｅｇ２７から受け取り、処理部２１から出力されたアドレスの各ビットと暗号化／復号化ＫＥＹの各ビットとに対してＥＯＲ演算を行うことにより、処理部２１から出力されたアドレスを暗号化する。

【０１０３】このように、暗号化ＥＯＲゲート列２９は、暗号化／復号化ＫＥＹに基づいて処理部２１から出力されたアドレスを暗号化する暗号化部として機能する。

【０１０４】次に、図６を参照して、記憶装置１とデータ処理装置２とを含むデータ転送システム１００の動作を説明する。

【０１０５】記憶装置１がデータ処理装置２に装着されると、ハードリセットが行われる。このハードリセットに応答して、制御部２０の暗号生成コントローラ２３は、「ＫＥＹリセット信号」を暗号化／復号化器２２に設けられたＫｅｙ＿Ｒｅｇ２７と暗号化／復号化器１１に設けられたＫｅｙ＿Ｒｅｇ１４に出力する（図６（ｂ））。その結果、Ｋｅｙ＿Ｒｅｇ１４およびＫｅｙ＿Ｒｅｇ２７に保持されるデータは、それぞれ、「ＡＬＬ０」にリセットされる（図６（ａ））。Ｋｅｙ＿Ｒｅｇ１４およびＫｅｙ＿Ｒｅｇ２７に保持されるデータが「ＡＬＬ０」であることは、暗号化／復号化ＫＥＹがリセットされた状態であることを示す。

【０１０６】Ｋｅｙ＿Ｒｅｇ１４に「ＡＬＬ０」が保持されると、セレクタ１６は、復号化ＥＯＲゲート列１５から出力されるアドレスにかかわらず、「０番地」のアドレスを記憶部１０に出力する。

【０１０７】記憶部１０は、「０番地」のアドレスに記憶されたＩＤ情報を出力する。ＩＤ情報は、暗号化ＥＯＲゲート列１７を介してデータ処理装置２に転送される。

【０１０８】このように、暗号化／復号化ＫＥＹがリセットされた状態と記憶部１０の「０番地」とを関連付けることにより、暗号化／復号化ＫＥＹがリセットされた状態において、記憶部１０の「０番地」以外のアドレスからデータが読み出されるおそれがない。

【０１０９】制御部２０の暗号生成コントローラ２３は、「ＩＤセット信号」をＩＤ＿Ｒｅｇ３６に出力する（図６（ｉ））。その結果、記憶装置１からデータ処理装置２に転送されたＩＤ情報がＩＤ＿Ｒｅｇ３６にセットされる（図６（ｈ））とともに、ＬＦＳＲ初期値特性多項式設定部２４に出力される。

【０１１０】ＬＦＳＲ初期値特性多項式設定部２４は、ＩＤ情報に基づいて、疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを決定する（図６（ｇ））。ＬＦＳＲ初期値特性多項式設定部２４は、疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを設定するための制御信号ＳＥＬＢＵＳをＬＦＳＲフィードバック等価論理形成部３１に出力する。

【０１１１】制御部２０の暗号生成コントローラ２３は、「初期値ロード信号」をＬＦＳＲ１２およびＬＦＳＲ２５に出力する（図６（ｅ））。

【０１１２】「初期値ロード信号」に応答して、ＬＦＳＲ１２のシフトレジスタ１８ａに初期値が設定され、ＬＦＳＲ２５のシフトレジスタ３０に初期値が設定される（図６（ｄ））。ここで、シフトレジスタ１８ａに設定される初期値は、ＩＤ情報に基づき予め設定されていた値であり、シフトレジスタ３０に設定される初期値は、ＩＤ情報に基づきＬＦＳＲ初期値特性多項式設定部２４によって演算により決定された値である。

【０１１３】制御部２０の暗号生成コントローラ２３は、「シフトクロック」をＬＦＳＲ１２およびＬＦＳＲ２５に出力する（図６（ｆ））。

【０１１４】「シフトクロック」に応答して、ＬＦＳＲ１２のシフトレジスタ１８ａに対してM_1回のシフト演算が行われ、ＬＦＳＲ２５のシフトレジスタ３０に対してM_1回のシフト演算が行われる（図６（ｄ））。

【０１１５】なお、ＬＦＳＲ１２では、１回のシフト演算を行う度に、ＬＦＳＲ特定多項式に基づく論理演算が行われる。そのＬＦＳＲ特性多項式は、ＩＤ情報に基づき予め設定されていた多項式である。その論理演算結果がシフトレジスタ１８ａの入力にフィードバックされる。同様にして、ＬＦＳＲ２５では、１回のシフト演算を行う度に、ＬＦＳＲ特定多項式に基づく論理演算が行われる。そのＬＦＳＲ特性多項式は、ＩＤ情報に基づきＬＦＳＲ初期値特性多項式設定部２４によって演算により決定された多項式である。その論理演算結果がシフトレジスタ３０の入力にフィードバックされる。

【０１１６】このように、ＬＦＳＲ１２および２５で

は、「シフトクロック」が入力される毎に、シフト演算と論理演算とが繰り返される。その結果、暗号化／復号化器１１および２２において全く同一の演算が行われる。

【０１１７】このように、ＬＦＳＲ１２には、ＩＤ情報に基づいて予め決定される疑似乱数を生成するための初期値とＬＦＳＲ特性多項式とを実現するための回路が予め組み込まれている。ＬＦＳＲ２５には、ＬＦＳＲ１２と等価論理を形成可能な仕組みが予め準備されており、ＬＦＳＲ初期値特性多項式設定部２４は、記憶装置１から転送されるＩＤ情報に基づいて、ＬＦＳＲ１２と等価論理を形成するようにＬＦＳＲ２５を構成する。

【０１１８】その結果、暗号化／復号化器１１における暗号化／復号化ＫＥＹと、暗号化／復号化器２２における暗号化／復号化ＫＥＹとは、同等の論理に従って生成される。

【０１１９】制御部２０の暗号生成コントローラ２３は、「シフトクロック」をＬＦＳＲ１２およびＬＦＳＲ２５に所定の回数だけ出力した後に、「ＫＥＹセットクロック」をＫｅｙ＿Ｒｅｇ１４およびＫｅｙ＿Ｒｅｇ２７に出力する（図６（ｃ））。

【０１２０】「ＫＥＹセットクロック」に応答して、ＬＦＳＲ１２から出力される出力データＯＵＴがＫｅｙ＿Ｒｅｇ１４に取り込まれ、そこに保持されるとともに、ＬＦＳＲ２５から出力される出力データＳＯＵＴがＫｅｙ＿Ｒｅｇ２７に取り込まれ、そこに保持される。

【０１２１】このようにして、Ｋｅｙ＿Ｒｅｇ１４とＫｅｙ＿Ｒｅｇ２７とに同一の暗号化／復号化ＫＥＹ（例えば、A_1''）が保持されることになる（図６（ａ））。

【０１２２】記憶装置１がデータ処理装置２に装着されている場合には、暗号化／復号化器１１と暗号化／復号化器２２とは、データバスとアドレスバスとを介して接続される。データバスを介して、暗号化／復号化ＫＥＹに基づいて暗号化されたデータが記憶装置１からデータ処理装置２に転送される（図６（ｊ））。アドレスバスを介して、暗号化／復号化ＫＥＹに基づいて暗号化されたアドレスがデータ処理装置２から記憶装置１に転送される（図６（ｋ））。

【０１２３】その後、処理部２１は、記憶装置１に記憶されたデータのうちデータ処理装置２によって処理されるべきデータを指定するアドレスを出力する。そのアドレスは、暗号化／復号化器２２の暗号化ＥＯＲゲート列２９に与えられる。

【０１２４】暗号化ＥＯＲゲート列２９は、アドレスの各ビットとＫｅｙ＿Ｒｅｇ２７に保持されている暗号化／復号化ＫＥＹの各ビットに対してＥＯＲ演算を行うことにより、アドレスを暗号化する。具体的には、暗号化／復号化ＫＥＹの複数のビットのうち「１」のビットに対応するアドレスのビットの論理（１／０）が反転される。暗号化されたアドレスは、暗号化／復号化器１１の復号化ＥＯＲゲート列１５に与えられる。

【０１２５】復号化ＥＯＲゲート列１５は、暗号化されたアドレスの各ビットとＫｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹの各ビットに対してＥＯＲ演算を行うことにより、暗号化されたアドレスを復号化する。具体的には、暗号化／復号化ＫＥＹの複数のビットのうち「１」のビットに対応する暗号化されたアドレスのビットの論理（１／０）が反転される。

【０１２６】Ｋｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹとＫｅｙ＿Ｒｅｇ２７に保持されている暗号化／復号化ＫＥＹとは同一である。従って、上述した態様で暗号化されたアドレスを復号化することにより、暗号化されたアドレスは元のアドレスに変換される。

【０１２７】復号化ＥＯＲゲート列１５から出力されるアドレスは、セレクタ１６に与えられる。セレクタ１６は、暗号化／復号化ＫＥＹがリセットされている状態であるか否かを判定する。Ｋｅｙ＿Ｒｅｇ１４に保持されているデータが「ＡＬＬ０」以外である場合には、セレクタ１６は、暗号化／復号化ＫＥＹがリセットされている状態ではないと判定する。この場合には、セレクタ１６は、復号化ＥＯＲゲート列１５から出力されるアドレスを記憶部１０に出力する。

【０１２８】記憶部１０は、アドレスに対応する位置に記憶されているデータを読み出し、読み出したデータを暗号化ＥＯＲゲート列１７に出力する。

【０１２９】暗号化ＥＯＲゲート列１７は、記憶部１０から出力されたデータの各ビットとＫｅｙ＿Ｒｅｇ１４に保持されている暗号化／復号化ＫＥＹの各ビットに対してＥＯＲ演算を行うことにより、記憶部１０から出力されたデータを暗号化する。具体的には、暗号化／復号化ＫＥＹの複数のビットのうち「１」のビットに対応するデータのビットの論理（１／０）が反転される。暗号化ＥＯＲゲート列１７による暗号化の原理は、暗号化ＥＯＲゲート列２９による暗号化の原理と同一である。暗号化されたデータは、暗号化／復号化器２２の復号化ＥＯＲゲート列２８に与えられる。

【０１３０】復号化ＥＯＲゲート列２８は、暗号化されたデータの各ビットとＫｅｙ＿Ｒｅｇ２７に保持されている暗号化／復号化ＫＥＹの各ビットに対してＥＯＲ演算を行うことにより、暗号化されたデータを復号化する。具体的には、暗号化／復号化ＫＥＹの複数のビットのうち「１」のビットに対応する暗号化されたデータのビットの論理（１／０）が反転される。復号化ＥＯＲゲート列２８による復号化の原理は、復号化ＥＯＲゲート列１５による復号化の原理と同一である。復号化ＥＯＲゲート列２８から出力されるデータは、処理部２１に与えられる。

【０１３１】処理部２１は、復号化ＥＯＲゲート列２８

から出力されるデータに対して所定の処理を実施する。

【０１３２】以後、記憶装置１とデータ処理装置２との間におけるデータの転送と並行して、新たな暗号化／復号化ＫＥＹを生成するための演算がＬＦＳＲ１２およびＬＦＳＲ２５において行われる。このような演算は、一定の時間毎に行われてもよいし、ランダムな時間毎に行われてもよい。

【０１３３】新たな暗号化／復号化ＫＥＹを生成するためにＬＦＳＲ１２およびＬＦＳＲ２５においてなされるシフト演算の回数（例えば、M_2回）は、前回の暗号化／復号化ＫＥＹを生成するためにＬＦＳＲ１２およびＬＦＳＲ２５においてなされるシフト演算の回数（例えば、M_1回）とは異なるように設定される（図６（ｄ））。

【０１３４】「ＫＥＹセットクロック」に応答して、Ｋｅｙ＿Ｒｅｇ１４およびＫｅｙ＿Ｒｅｇ２７に保持されている暗号化／復号化ＫＥＹが更新される（図６（ａ））。その後、新たな暗号化／復号化ＫＥＹに基づいて暗号化されたアドレスと暗号化されたデータとが記憶装置１とデータ処理装置２との間で転送される（図６（ｊ）、図６（ｋ））。

【０１３５】このように、暗号化／復号化器１１のＫｅｙ＿Ｒｅｇ１４に保持された暗号化／復号化ＫＥＹと暗号化／復号化器２２のＫｅｙ＿Ｒｅｇ２７に保持された暗号化／復号化ＫＥＹとは、「ＫＥＹセットクロック」に応答して、同時に、しかも、瞬時に、新たな暗号化／復号化ＫＥＹに更新される。従って、暗号化／復号化ＫＥＹを書き換える際にも、記憶装置１とデータ処理装置２との間でデータ転送を中断する必要がなく、連続してデータ転送することができる。

【０１３６】なお、本発明は、上述の実施の形態に限らず、種々に変更してもよい。上記の実施の形態では、ＩＤ情報以外のすべてのアドレスおよびデータを暗号化して転送しているが、データ処理装置２に不正な記憶装置１が接続された場合のシステムの異常な動作を回避するために、基礎的なプログラム領域などのデータ要求時には、アドレスおよびデータの暗号化を行わないようにしてもよい。

【０１３７】また、上記の実施の形態では、データ処理装置２は、１つの記憶装置１だけが接続されてデータが処理される構成であったが、データ処理装置２に対して、同時に複数の記憶装置１が接続可能であって、複数の記憶装置１から選択した１つの記憶装置１との間にて転送されるデータのみを暗号化／復号化するようにしてもよい。

【０１３８】さらに、上記の実施の形態では、記憶装置１の記憶部１０の「０番地」のアドレスに記憶装置１に固有のＩＤ情報を記憶するようにしているが、記憶装置１の記憶部１０以外に、ＩＤ情報を格納する部分を設けるようにしてもよい。

【０１３９】記憶装置１に固有のＩＤ情報は、品番等のＩＤ番号に限らず、ＬＦＳＲの初期値および特性多項式を設定することに使用可能ならば、どのようなものであってもよい。

【０１４０】

【発明の効果】本発明のデータ転送システムによれば、記憶装置とデータ処理装置との間で転送されるアドレスおよびデータが暗号化されている。このため、転送データから記憶装置に記憶されたデータの内容を知ることは容易ではない。これにより、記憶装置に記憶されたデータが不正に複製されることを防止することができる。

【０１４１】また、本発明のデータ転送システムによれば、転送データの暗号化および復号化に使用される暗号化／復号化ＫＥＹは、データ処理装置に装着された記憶装置のＩＤ情報に対応するように生成される。このため、仮に記憶装置に記憶されているデータがそのまま複製されたとしても、記憶装置のＩＤ情報に基づいて暗号化／復号化ＫＥＹを生成し、暗号化／復号化ＫＥＹに基づいてデータを暗号化する仕組みを付加しない限り、データ処理装置は、その複製データを正しく読み取ることができない。これにより、記憶装置に記憶されたデータが不正に複製使用されることを防止することができる。

【０１４２】記憶装置には、ＩＤ情報に基づいて暗号化／復号化ＫＥＹを生成するための初期値および特性多項式が予め回路として作り込まれている。これにより、初期値および特性多項式を生成するための回路等が不要になる。その結果、記憶装置の小規模化を実現することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態のデータ転送システム１００の構成例を示す図である。

【図２】記憶装置１の暗号化／復号化器１１の構成例を示す図である。

【図３】ＬＦＳＲ１２の構成例を示す図である。

【図４】データ処理装置２の暗号化／復号化器２２の構成例を示す図である。

【図５】（ａ）はシフトレジスタ３０およびＬＦＳＲフィードバック等価論理形成部３１の構成例を示す図、（ｂ）はＬＦＳＲフィードバック等価論理形成用ゲート素子３３の構成例を示す図である。

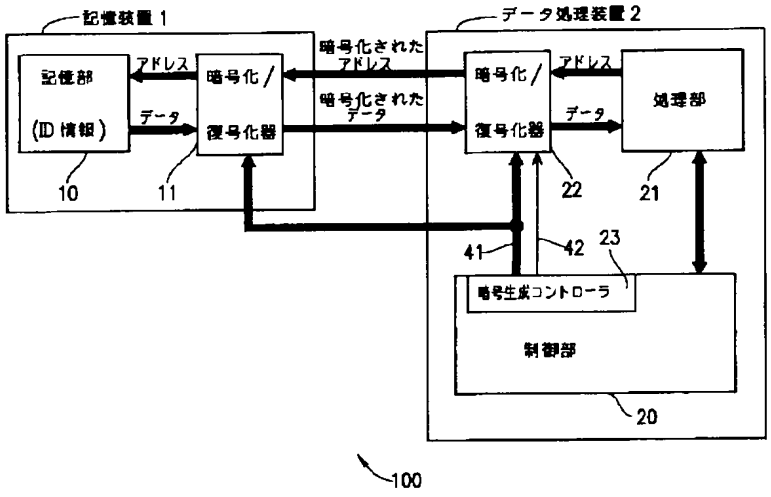
【図６】データ転送システム１００の動作を説明するタイミングチャートである。

【符号の説明】

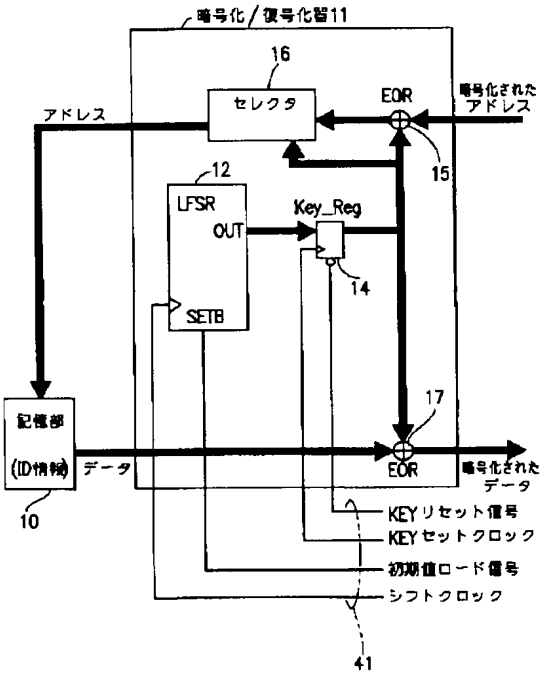
１　　記憶装置
２　　データ処理装置
１０　記憶部
１１　暗号化／復号化器
１２　ＬＦＳＲ
１４　Ｋｅｙ＿Ｒｅｇ
１５　復号化ＥＯＲゲート列

１６　セレクタ
１７　暗号化ＥＯＲゲート列
２０　制御部
２１　処理部
２２　暗号化／復号化器
２３　暗号生成コントローラ
２４　ＬＦＳＲ初期値特性多項式設定部
２５　ＬＦＳＲ
２７　Ｋｅｙ＿Ｒｅｇ
２８　復号化ＥＯＲゲート列
２９　暗号化ＥＯＲゲート列
３０　シフトレジスタ
３１　ＬＦＳＲフィードバック等価論理形成部
３２　セットリセット付きＤフリップフロップ
３３　ＬＦＳＲフィードバック等価論理形成用ゲート素子
３４　ＥＯＲ演算素子
３５　４－１セレクタ
３６　ＩＤ＿Ｒｅｇ

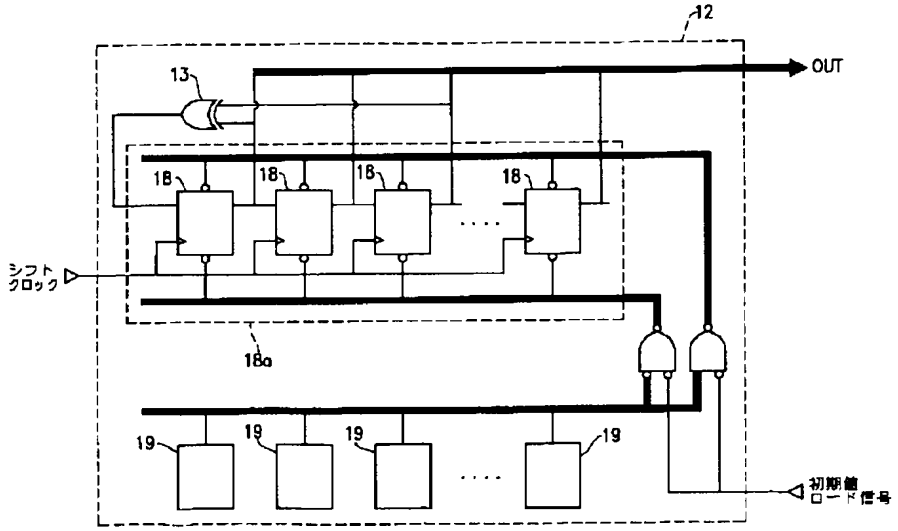
【図１】



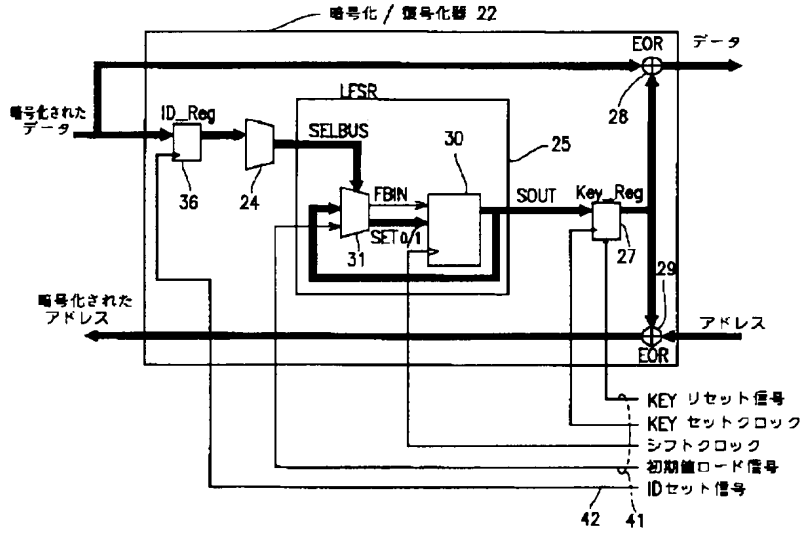
【図２】



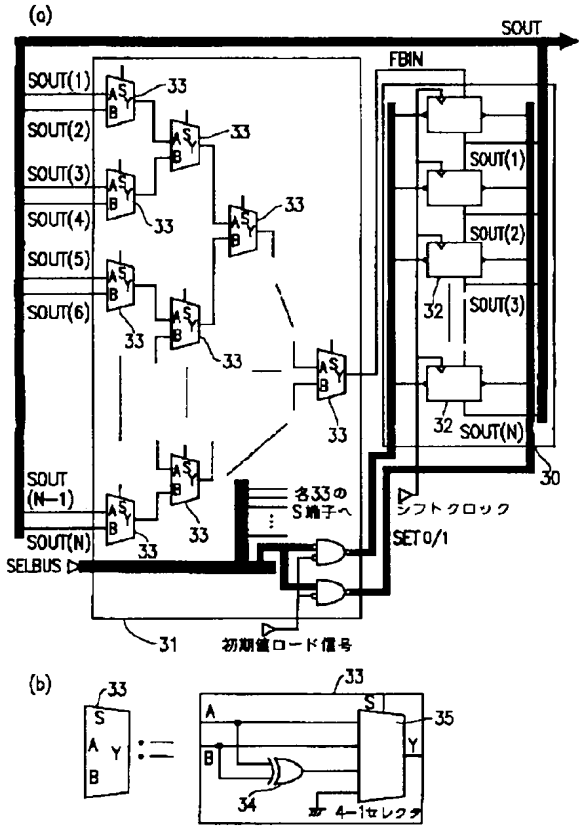
【図３】


12
OUT
13
18
18
18
18
シフトクロック
18a
19
19
19
19
初期値ロード信号

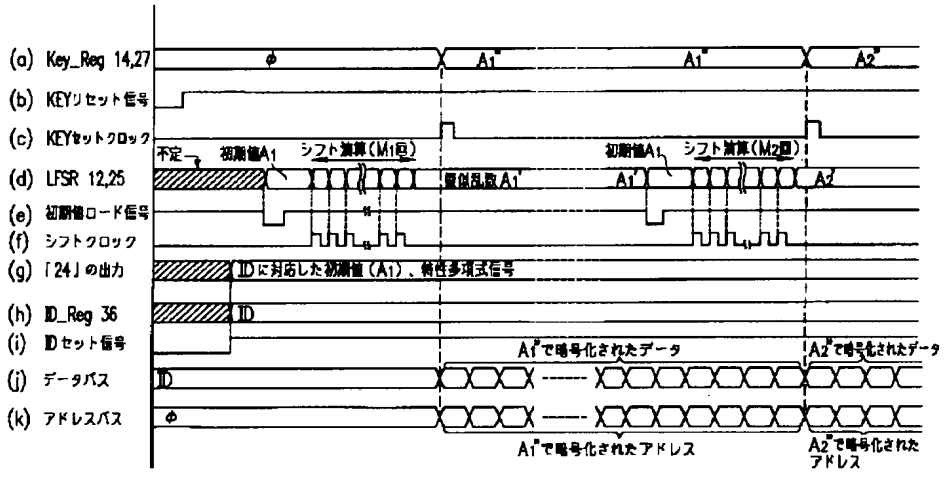
【図４】


暗号化／復号化器 22
EOR
データ
暗号化されたデータ
ID_Reg
LFSR
SELBUS
30
25
28
36
24
FBIN
SDOUT
Key_Reg
SET 0/1
31
27
29
暗号化されたアドレス
アドレス
EOR
KEY リセット信号
KEY セットクロック
シフトクロック
初期値ロード信号
IDセット信号
42
41

【図５】


(a)
SOUT
FBIN
SOUT(1)
SOUT(2)
SOUT(3)
SOUT(4)
SOUT(5)
SOUT(6)
SOUT(N-1)
SOUT(N)
SELBUS
33
32
30
31
名33のS端子へ
シフトクロック
SET 0/1
初期値ロード信号
(b)
S
A
B
Y
34
35
4-1セレクタ

【図６】


(a) Key_Reg 14,27
(b) KEYリセット信号
(c) KEYセットクロック
(d) LFSR 12,25
(e) 初期値ロード信号
(f) シフトクロック
(g) 「24」の出力
(h) ID_Reg 36
(i) IDセット信号
(j) データバス
(k) アドレスバス
φ
A1'
A2'
不定
初期値A1
シフト演算(M1回)
初期値A1'
シフト演算(M2回)
IDに対応した初期値(A1')、特性多項式信号
ID
A1'で暗号化されたデータ
A2'で暗号化されたデータ
A1'で暗号化されたアドレス
A2'で暗号化されたアドレス